N COVERING CODES AND COVERING RADIUS OF SOME OPTIMAL CODES

by

C. DURAIRAJAN

DEPARTMENT OF MATHEMATICS

INDIAN INSTITUTE OF TECHNOLOGY KANPUR

March, 1996

ON COVERING CODES AND COVERING RADIUS OF SOME OPTIMAL CODES

A thesis Submitted
in Partial Fulfilment of the Requirements
for the Degree of

DOCTOR OF PHILOSOPHY

by

C. DURAIRAJAN

to the

DEPARTMENT OF MATHEMATICS

INDIAN INSTITUTE OF TECHNOLOGY KANPUR

March, 1996

CERTIFICATE

It is certified that the work contained in the thesis entitled **"ON COVERING CODES AND COVERING RADIUS OF SOME OPTIMAL CODES"**, by **C. Durairajan** for the award of Degree of Doctor of Philosophy at the Indian Institute of Technology, Kanpur has been carried out under my supervision. To the best of my knowledge this work has not been submitted elsewhere for a degree.

M Bhandari

(Prof. M. C. Bhandari)
Thesis Supervisor
Department of Mathematics
Indian Institute of Technology
Kanpur-208 016
India

March, 1996.

ACKNOWLEDGEMENT

I wish to express my gratitude to my thesis supervisor, Prof. M. C. Bhandari, for his guidance and encouragement. I am extremely thankful to him for the patience he has shown in guiding and going through my work. I also thank Prof. H. Janwa and Dr. A. K. Lal for their help and advice during the period of my visit at MRI, Allahabad. I am grateful to my senior, Dr. Madhusudan Garg, for many valuable discussions and timely helps.

I take this opportunity to thank with pleasure, Professors S. P. Mohanty, R. K. S. Rathore, U. B. Tewari, V. Raghavendra, Dr. P. Shanmugaraj, Dr. A. K. Lal and all other members of the department of mathematics, IIT Kanpur for their kindly help and valuable suggestions.

I owe a lot to my friends Alphonse, Sokkalingam, Balram, Miss. Padmasundari, Sundararajan who were ever present with their unfailing encouragement and help at all my moments of stress and made my job easier. I express my sincere thanks to my colleagues Chanduka, Manish and Nemate for useful discussion on the subject. It will be difficult for me to forget friends like Govind, Tamil, Kalyanaraman (both), Sivaguru, Arumugam, Guruprem, Venky, Sini, Sivakumar, Balaji and Rajesh (both).

Any amount of words will be inadequate to describe the love and support that my parents and my family members have given to me and the sacrifices they have made. They alone have initiated, inspired and finally have given the courage and strength to undertake and complete the task. Last, but not the least, and many more who made my stay at IIT Kanpur a memorable one.

C. Durairajan.

CONTENTS

CHAPTER PAGE

Nomenclature

F_q	Finite field if q is a prime power otherwise integer modulo q.
$GF(q)$	Galois field with q elements.
F_q^n	The set of all n-tuples over F_q .
$w(x)$	Weight of the vector x.
$\|S\|$	Cardinality of the set S.
$d(x,y)$	Hamming distance between the vectors x and y.
$d(x,S)$	Distance between the vector x and the set S.
$<x,y>$	Inner product of x and y.
$[n, k, d]$	A linear code of length n, dimension k and minimum distance d.
$(q, n, M)R$	A q-ary code of length n and codewords M with covering radius R.
$A\oplus B$	Direct sum of A and B.
$A\dot{\oplus}B$	Amalgamated direct sum of A and B.
$[A\backslash B]$	Matrix obtained by deleting columns of the matrix B from the matrix A.
x^t	Transpose of the vector x.
A^t	Transpose of the matrix A.
$S_k(q)$	k-dimensional q-ary Simplex code.
$G_k(q)$	Generator matrix of a k-dimensional q-ary Simplex code.
$C_{k,u}(q)$	k-dimensional q-ary MacDonald code.
$G_{k,u}(q)$	Generator matrix of a k-dimensional q-ary MacDonald code.

$C^{\perp}$	Dual of a code C.
A_i	Number of i weight codewords in C.
B_i	Number of i weight codewords in $C^{\perp}$.
$R(C)$	covering radius of the code C.
$\lfloor x \rfloor$	The greatest integer less than or equal to x.
$\lceil x \rceil$	The smallest integer greater than or equal to x.
$\binom{n}{r}$	The combinations of n things taken r at a time.
$g_q(k,d)$	$\equiv \sum_{i=0}^{k-1} \lceil d/q^i \rceil$.
$n_q(k,d)$	The minimal length of a q-ary linear code of dimension k and minimum distance d.
$K_q(n,R)$	Minimum cardinality of a q-ary code of length n and covering radius R.
$t_q[n,k]$	The minimum covering radius of a q-ary linear code of length n and dimension k.
$l(m, R; q)$	The minimum length of a q-ary code with codimension m and covering radius R.
$Res(C,c)$	Residual code of C with respect to the codeword $c \in C$.
$Res(C,w)$	Residual code of C with respect to a codeword of weight w.
$C_{\alpha}^{(i)}$	The set of codewords of a code whose ith coordinate is α.
$b_q(k,d)$	$\equiv n_q(k+1,d) - n_q(k,d)$.

(m,n)	Greatest common divisor of m and n.
■	End of a proof.

Synopsis

Name of the Student : **C. Durairajan** Roll No. : **9010863**

Degree for which submitted : **Ph. D.** Department : **Mathematics**

Thesis Title : **On Covering Codes and Covering Radius of Some Optimal Codes**

Name of the thesis supervisor : **Prof. M. C. Bhandari**

Month and year of thesis submission : **February, 1996**

Let F_q be a set of alphabets consisting of q elements. If q is a prime power, we take $_q$ to be the Galois field GF(q), otherwise F_q is Z_q, the set of integers modulo q. A code C s a nonempty subset of $F_q^n, n \geq 1$. If C is in addition a subspace of F_q^n, then C is called a -ary linear code. A linear code of length n, dimension k and minimum distance d is called n [n, k, d] q-ary code. If q = 2, the code is called a binary code.

For a given k and d, let $n_q(k,d) = \min\{n \mid$ there exists an $[n,k,d]$ q-ary code $\}$. n 1965, Solomon and Stiffler [14] have shown that

$$n_q(k,d) \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil \equiv g_q(k,d)$$

here $\lceil x \rceil$ denotes the smallest integer greater than or equal to x. For binary case q = 2, the bove inequality was first proved by Griesmer [6] and is popularly know as Griesmer bound. n $[n_q(k,d),k,d]$ code is called an optimal code and a $[g_q(k,d),k,d]$ code, if it exist, is alled a code meeting the Griesmer bound.

Another important parameter of a code is its covering radius. The covering radius of code C is the least integer R such that spheres of radius R around the codewords cover the hole space. It is denoted by R(C). A code C that has no super code with same minimum istance d is characterized by $R(C) \leq d-1$. If the code is used for data compression, the overing radius is a measure of the maximum distortion; if for error correction, then R(C) s the maximum weight of a correctable random error. Many alternate criterions for the overing radius are known [2].

A q-ary code of length n with M codewords and covering radius R is called a (q, n, M)R code. For a given n and R, let $K_q(n, R) = \min\{M \mid$ there is a $(q, n, M)R$ code $\}$. The problem of determining the value of the $K_q(n, R)$ is known as the covering problem. For q = 3 and R = 1, the problem is popularly known as the "football pool problem".

Determining $K_q(n, R)$, in general is a difficult task. In recent year many researchers viz, van Wee [15], Honkala [9], Ostergard [13] etc are actively working on determining bounds for $K_q(n, R)$. The researchers have introduced different kinds of partitioning properties of the codes to improve upon direct sum construction using other sum constructions. The concepts of normal and subnormal binary codes were introduced in [5] and [9], respectively and these concepts were later generalized by Lobstein and van Wee [12] to q-ary codes. n 1991, Ostergard introduced the concept of seminormal and strongly seminormal code to get further improvement on the upper bound for $K_q(n, R)$ and conjectured that (5, 6. 25)3 and (5, 6, 125)2 strongly seminormal codes exist.

The present dissertation determines:

1. Better bounds for $K_q(n, R)$.

2. Bounds on $n_q(k, d)$ for k = 3, 4 and some d and $n_4(5, d)$.

3. Bounds on the covering radius of q-ary Simplex and MacDonald codes.

Chapter I and Chapter II contains an introduction and a brief survey of known result. n Chapter III, we determine a necessary and sufficient conditions for an optimal code to be trongly seminormal. Construction of a $(q, q+1, q^2)q-2, q \geq 4$, strongly seminormal and ome other strongly seminormal codes are given. This proves Ostergard's conjecture and also helps to prove the following theorem.

Theorem 1. $K_q(n+q, R+q-2) \leq qK_q(n, R)$ *for* $q \geq 4$,

$K_5(n+5, R+3) \leq 5K_5(n, R)$,

$K_3(n+10, R+6) \leq 9K_3(n, R)$.

Above theorem improves many upper bounds on $K_q(n,R)$ for q = 3, 5 and some n and R. The following result gives another upper bound on $K_q(n,R)$.

Theorem 2. *If there exists a (q,n,M)R seminormal code, then* $K_q(n+q, R+q-1) \leq M$.

A similar theorem (Theorem 2, [10]) with stronger hypotheses was proved by Honkala. However, our proof is much simpler than his proof.

The following observation gives a lower bound to $K_q(n,R)$ and improves previous known lower bounds for some n and R.

Theorem 3.

$$K_q(\sum_{i=1}^{t} n_i, \sum_{i=1}^{t} R_i + (t-1)) \geq \min_i\{K_q(n_i, R_i)\} \textit{ for } n_i \geq 1 \textit{ and } 0 \leq R_i \leq n_i.$$

Using Theorem 3 and a result of Ostergard (Theorem 6, [13]), it is observed that $K_3(6n, 4n-1) = 6$ for $n \geq 1$ and $K_q(q, q-2) \leq K_q(qr, qr-r-1) \leq 2q$ for all $r \geq 1$ and $q \geq 2$. As a consequence, we get $K_2(2r, r-1) = 4$; a result of Cohen et al [1]. In case $q \geq 3$ and $R = q-2$, the following theorem further improves this bound.

Theorem 4. *If* $q \geq 3$, *then* $K_q(q, q-2) \leq 2q-1$.

In recent years many researchers have determined $n_2(k,d)$ for $k \leq 8$ and bounds on $n_2(9,d)$. But very little is known for q-ary codes in general. It has been shown independently by Dodunekov [3] and Hamada and Tamari [7] that $n_q(2,d) = g_q(2,d)$. Necessary and sufficient conditions for a q-ary code to meet the Griesmer bound and some elementary properties have been obtained by Dodunekov [3] and Hill [8]. In [3], Dodunekov has determined $n_q(3,d)$ for $d \leq q+2$. An attempt to determine $n_q(k,d)$, in general for k = 3 and 4 is done in Chapter IV. The following theorem gives bound on $n_q(3,2q)$. |

Theorem 5. *(i) If q is even, then* $n_q(3,2q) = g_q(3,2q)+1$.

(ii) If q is odd and $3 \not| q$, *then* $g_q(3,2q)+1 \leq n_q(3,2q) \leq g_q(3,2q)+2$.

It is conjectured that $n_q(3,2q)$ reaches the lower bound given by Theorem 5. It is supported by a result of Hill [8] for q = 5 and 7 and by numerous examples constructed by us. The following two theorems determine the value of $n_q(4,d)$ for $d = q(q-2)$ and some other values.

Theorem 6. *For* $q \geq 4$, $n_q(4,q(q-2)) = g_q(4,q(q-2)) + 1$.

Theorem 7. *(i) If q is odd, then* $n_q(4,q^2-i) = g_q(4,q^2-i)+1$ *for* $1 \leq i \leq q-1$.
(ii) If q is even, then $n_q(4,q^2-i) = g_q(4,q^2-i)+1$ *for* $0 \leq i \leq 2$.

To obtain a lower bound for $n_q(k,d)$, we prove the following theorem.

Theorem 8. *If* $n_q(k,d) \geq g_q(k,d)+t, t \geq 0$, *then* $n_q(k+1,qd-i) \geq g_q(k+1,qd-i)+t, 0 \leq i \leq q-1$.

In particular if q =4 and k = 5, we get

Theorem 9. $n_4(5,d) \geq g_4(5,d)+1$ *for* $d = 3,4,20,187,188, 7 \leq d \leq 16, 23 \leq d \leq 32, 35 \leq d \leq 64, 77 \leq d \leq 80, 89 \leq d \leq 128, 145 \leq d \leq 176, 305 \leq d \leq 320$.

The last chapter is devoted to determining the upper and lower bounds for the covering radius of q-ary Simplex and MacDonald codes. Let $S_k(q)$ denotes the q-ary k-dimensional Simplex code. It is known that $R(S_k(2)) = 2^{k-1}-1$. For $q > 2$, very little is known about $R(S_k(q))$. In [11], Janwa has posed this as an open problem. It has been independently shown by Dodunekov [3] and Janwa [11] that

$$R(S_k(q)) \leq q^{k-1} - 1. \tag{1}$$

In [4], Garg has shown that the bound given by (1) is reached for k = 2 and q even. He also improves this bound for q = 3 and 4. Lower and upper bounds for $R(S_k(3)), R(S_k(4))$ and $R(S_k(5))$ are also obtained. But these are not good bounds and we further improve upon them. The following theorem gives exact value of $R(S_2(q))$ for q odd and $R(S_3(q))$ for even q.

Theorem 10. $R(S_2(q)) = q - 2$ for q odd,

$$R(S_3(q)) = \begin{cases} q^2 - 2 & \text{for q even} \\ q^2 - 3 \text{ or } q^2 - 2 & \text{for q odd.} \end{cases}$$

In case $R(S_m(q))$ is known for some m, the following theorem gives a better upper bound on $R(S_k(q))$, for $k \geq m$.

Theorem 11. If for some m and q, $R(S_m(q)) \leq q^{m-1} - t, t \geq 1$, then $R(S_k(q)) \leq q^{k-1} - t$, for all $k \geq m$.

We also show that $R(S_4(3)) = 24$ and $R(S_4(4)) = 61$. The bound given by (1) is further improved

Theorem 12. (i) $R(S_k(q)) \leq q^{k-1} - 2$, for $k \geq 3$.

(ii) $R(S_k(q)) \leq q^{k-1} - 3$, for $k \geq 4$ and $q = 3, 4$.

If $(k, q-1) = 1$, then $S_k(q)$ is a cyclic code. Using cyclic code properties, the following lower bounds are obtained for particular k and q = 3 and 4.

Theorem 13. i) If k is odd, then $R(S_k(3)) \geq 3^{k-1} - (\sqrt{3^{k-1}} + 1)/2$.

ii) If $3 \not| k$, then

$$R(S_k(4)) \geq \begin{cases} 4^{k-1} - (2^{k-1} + 1)/3 & \text{k even} \\ 4^{k-1} - (2^{k-1} + 2)/3 & \text{k odd.} \end{cases}$$

Another important optimal code is the MacDonald code $C_{k,u}(q), u \leq k$, which is obtained by puncturing the code $S_u(q)$ from the code $S_k(q)$ [3]. For q = 2, Garg [4] has found the exact covering radius of $C_{k,u}(2)$ for u = 1, 2. For $q > 2$, almost nothing is known except the simple upper bound $R(C_{k,u}(q)) \leq q^{k-1} - q^{u-1} - 1$. The following theorem gives the covering radius of some MacDonald codes.

Theorem 14. $R(C_{2,1}(q)) = q - 2, R(C_{3,2}(q)) = q^2 - q - 1$ *and* $R(C_{3,1}(q)) = q^2 - 3$.

An upper bound for $R(C_{k,u}(q))$ is given by the following theorem

Theorem 15. *i) If $u \geq 3$, then $R(C_{k,u}(q)) \leq q^{k-1} - q^{u-1} - 2$.*

ii) $R(C_{k,u}(q)) \leq R(C_{m,u}(q)) + q^{m-1}(q^{k-m} - 1)$.

For particular q, k and u, we show that $R(C_{4,3}(3)) = 16, R(C_{4,1}(3)) = 24$ and $R(C_{4,2}(q)) \leq q^3 - q - 2$. Using these and Theorem 15, it is observed that

Theorem 16. $R(C_{k,2}(q)) \leq q^{k-1} - q - 2$ *and* $R(C_{k,1}(3)) \leq 3^{k-1} - 4$ *for* $k \geq 4$.

A lower bound for $R(C_{k,u}(q))$ is given by the following theorem

Theorem 17. $R(C_{k,u}(q)) \geq R(C_{k,k-1}(q)) + R(C_{k-1,u}(q))$.

It is also observed that

$$R(S_k(q)) \geq R(C_{k,k-1}(q)) + R(S_{k-1}(q)).$$

Reference

1. G. D. Cohen, A. C. Lobstein and N. J. A. Sloane, "Further Results on the Covering radius of codes", IEEE Trans. Inform. Theory, Vol. IT-32, pp. 680–694, 1986.

2. G. D. Cohen, M. R. Karpovsky, H. F. Mattson. Jr., and J. R. Schatz, "Covering Radius–Survey and Recent Results", IEEE Trans. Inform. Theory, Vol. IT-31, pp. 328–343, 1985.

3. S. M. Dodunekov, "Minimal block length of a linear q-ary code with specified dimension and code distance", Problems Information Transmission, Vol. 20, pp. 239–249, 1985.

4. M. S. Garg, "On Optimum codes and Their covering radii", Ph. D. Thesis, IIT Kanpur(India), 1990.

5. R. L. Graham and N. J. A. Sloane, "On the covering radius of codes", IEEE Trans. Inform. Theory, Vol. IT-31, pp. 385–401, 1985.

6. J. H. Griesmer, "A bound for error-correcting codes", IBM J. Res. Develop., Vol. 4, pp. 532-542, 1960.

7. N. Hamada and F. Tamari, "Construction of optimal codes and optimal fractional factorial designs using linear programming", Ann. Discrete Math., Vol.6, pp.175–188, 1980.

8. R. Hill, "Optimal linear codes", In C. Mitchell. ed., Proc. 2nd IMA Conf. on Cryptography and Coding (Oxford Univ. Press, Oxford, pp. 75–104, 1992.

9. I. S. Honkala, "Lower Bounds for Binary Covering codes", IEEE Trans. Inform. Theory, Vol. 34, No. 2, pp. 326–329, 1988.

10. I. S. Honkala, "On (k, t)-subnormal covering codes", IEEE Trans. Inform. Theory, Vol. 37, No. 4, pp. 1203–1206, 1991.

11. H. Janwa, "Some new upper bounds on the covering radius of binary linear codes", IEEE Trans. Inform. Theory", Vol. IT-35, pp. 110–122, 1989",

12. A. C. Lobstein and G. J. M. van Wee, "On Normal and subnormal q-ary covering codes", IEEE Trans. Inform. Theory, Vol. 35, No. 6, pp. 1291-1295, 1989

13. P. R. J. Ostergard, "Upper Bounds for q-ary covering codes", IEEE Trans. Inform. Theory, Vol. 37, No. 3, pp. 660–664, 1991.

14. G. Soloman and J. J. Stiffler, "Algebraically punctured cyclic codes", Information and Control, Vol. 8, pp. 170-179, 1965.

15. G. J. M. Van Wee, "Improved Sphere Bounds on the covering radius of codes", IEEE Trans. Inform. Theory, Vol. 34, pp. 237–245, 1988.

Chapter I

Introduction

Codes are designed to correct and detect errors while sending messages through a noisy communication channel as quickly and as reliably as possible. This originated from the classical paper of Shannon [52] in 1948. Due to noise, messages may be distorted. So the object of a code is to encode the data, by adding a certain amount of redundancy to messages, so that the original message can be recovered if a limited number of errors have occurred. Thus a code is a set of sequences, called codewords, of elements from a fixed set $F_q = \{ \alpha_1, \alpha_2, \cdots, \alpha_q\}$ of q alphabets. For making computations it is desirable that F_q has some algebraic structure. If q is a prime power, we take F_q to be a Galois field otherwise F_q is taken to be the set of integers modulo q. If every codeword has same length n, then the code is a subset of F_q^n and is called a **block code.** A code C containing M codewords of length n and minimum distance d (any two distinct codewords differ in at least d coordinates) is called an (n,M,d) q-ary code. If in addition C is a k-dimensional subspace of F_q^n , then C is called an [n, k, d] q-ary linear code.

The spheres of radius [(d-1)/2] around the codewords are mutually disjoint. So by using nearest neighbourhood decoding, one can correct at most [(d-1)/2] errors. A good code should have small n for fast transmission of messages, large k to send wide variety of messages and large d to correct more errors. These are conflicting goals. A central problem in coding theory is to optimize one of the parameters n, k, d for given values of the other two. These problems are equivalent [19]. The problem of determining $n_q(k, d)$, the minimum value of n for given k and d, is more natural because the Griesmer bound provides an important lower bound on $n_q(k,d)$. The $[n_q(k,d), k, d]$ code is called an **optimal** code. In recent years many researchers viz Baumert and McEliece [1], Tilborg [59], Dodunekov and Manev [16] Hill with Greenough [21] and Newton [30], Bhandari and Garg [5] have determined $n_q(k,d)$ for smaller value of q and k.

The spheres of radius $[(d-1)/2]$ around the codewords may not cover the whole space. The least nonnegative integer R such that spheres of radius R around the codewords cover the whole space is called the covering radius of the code. Note that R is the maximum number of correctable random errors. Determining covering radius of a code is in general a difficult task. During last two decades researchers have tried to improve upon the known lower and upper bounds for the covering radius and hence determining the covering radius of certain codes.

Another important problem of the coding theory is to determine $K_q(n, R)$, the minimum number of codewords in a q-ary code of length n and covering radius R. It is known as the covering problem. If q = 3 and R = 1, this is popularly known as the "football pool problem". In recent years Honkala [31], van Wee [61], Ostergard [48] and others have determined lower and upper bounds on $K_q(n, R)$ that are better than earlier known bounds.

The present dissertation aims to determine:

1. Bounds on $K_q(n,R)$.
2. Bounds on $n_q(k,d)$ for $k = 3$ and 4 and some d.
3. Covering radius of some optimal codes-the Simplex and the MacDonald codes.

The present dissertation is divided in to 5 Chapters. The Chapter II contains a brief survey of definitions and known results on optimal codes, covering radius of a code and covering codes. Chapter III deals with Problem 1 above. Few strongly seminormal codes are constructed. Existence of some of these codes was conjectured by Ostergard [47]. These also help in getting better upper bounds for $K_q(n,R)$. A lower bound to $K_q(n,R)$ is obtained by determining a relation between covering radii of known codes to the covering radius of their concatenation. It is seen that these bounds give 12 improvement in the latest tables given by Ostergard [47] and also help in getting exact value of $K_q(n,R)$ for certain n and R. A necessary and sufficient condition for an optimal code to be strongly seminormal is given.

Chapter IV is devoted to determining $n_q(k, d)$ for some k and d. A general lower bound on $n_q(k, d)$ is obtained. When applied to the case $q = 4$ and $k = 5$, it gives a lower bound on $n_4(5, d)$ that are better than the Griesmer bound. Exact value of $n_4(5, d)$ for small d are obtained by constructing suitable codes.

In [19] Garg has determined the covering radius of $S_2(q)$ for q even and has obtained lower and upper bounds of the covering radius of a Simplex code $S_k(q)$ in general. In Chapter V, we improve upon the bounds given by him and determine the covering radius of $S_2(q)$ for q odd and $S_3(q)$ for q even and some other ternary and quaternary Simplex codes. A well known example of an optimal code is the MacDonald code $C_{k,u}(q)$. $C_{k,u}(q)$ is generated by the matrix obtained from a generator matrix of $S_k(q)$ by deleting columns corresponding to $S_u(q)$. In [19] Garg has determined the covering radius of a binary MacDonald code for k = 3, 4. In the second part of Chapter V, we determine lower and upper bounds for the covering radius of $C_{k,u}(q)$ in general. Exact covering radius of $C_{k,u}(q)$ for k = 2, 3, $C_{4,1}(3)$ and $C_{4,3}(3)$.

Chapter II

Preliminaries and Survey

A nonempty set F with two binary operations '+', '.', popularly called addition and multiplication, is a **Field** if (i) (F, +) is an abelian group (ii) (F\{0}, .) is an abelian group and (iii) distributive laws hold. If in addition F is a finite set, F is called a **finite field**. A finite field with q elements exists if and only if $q = p^m$ for some prime number p and for some positive integer m. Moreover any two finite fields are isomorphic if and only if they have same number of elements. A finite field with q elements is called the **Galois field** and is denoted by GF(q).

Let F_q be an alphabet consisting of q elements. If q is a prime power, F_q is taken as the Galois field GF(q); otherwise $F_q = \mathbb{Z}_q$, the set of integers modulo q. Throughout this present dissertation $F_q = \{ \alpha_1 = 0, \alpha_2 = 1, \alpha_3, \cdots, \alpha_q \}$. Let $F_q^n = \{ x = (x_1, x_2, \cdots, x_n) \mid x_i \in F_q \}$. If F_q is a field, then F_q^n is an n-dimensional vector space over F_q . A code C is a nonempty subset of F_q^n. The elements of C are called **codewords** and n, the length of any codeword is called the length of C. For x, y $\in F_q^n$ the weight of x, denoted by w(x), is the number of non-zero coordinates of x and the distance between x and y, denoted by

,y), is the number of coordinate positions in which x and y fer. d(x,y) = w(x-y) is a metric on F_q^n and is known as Hamming tance. A subspace of F_q^n with Hamming distance is called a **ming space**. The minimum distance d of a code C is the smallest the distances between any two distinct codewords.

A code C of length n with M codewords and minimum distance d r F_q is called an (n, M, d) q-ary code. If q is a prime power . in addition C is subspace of F_q^n , then C is called a **linear .e**. A linear code of length n, dimension k and minimum distance ›ver F_q is called an [n, k, d] (or simply an [n, k], if we do wish to specify d) code. In linear codes, the minimum tance is the minimum weight of a nonzero codeword. A linear .e C of dimension k contains q^k codewords and can be described either (i) giving a basis for it or (ii) giving an (n-k)xn .rix H whose solution space is C. The matrix H is called a **·ity check matrix** of C and a k x n matrix G whose rows from a :is for C is called a **generator matrix**. Since the rank of H n - k, C contains a codeword of weight n - k + 1 and hence

1)
$$d \leq n - k + 1$$

:re d is the minimum distance of C.

The bound given by (2.1) is known as the **singleton bound**. If = n - k + 1, then C is called a **Maximum Distance Separable)S)** code. A code C_1 is a **subcode** (**Super code**) of C if $C_1 \subseteq C$ $\supseteq$ C). If no proper super code of a given code C with same ıimum distance exists, then C is called a **maximal code**.

Two (n, M, d) codes C and D are said to be **equivalent** if one can be obtained from the other by applying finitely many operations of the type:

i) permutation of coordinates,

ii) adding a fixed vector to each codeword,

iii) multiplying one or more coordinates by nonzero elements of F_q .

Let $x, y \in F_q^n$. The inner product of x and y, denoted by $<x,y>$, is $\sum_{i=1}^n x_i y_i$. If C is a q-ary code of length n, the code $C^\perp = \{ x \in F_q^n \mid <x,c> = 0$ for all $c \in C \}$ is called the **dual code** of C. If C is an [n, k] code, then $C^\perp$ is an [n, n-k] code. Moreover G is a generator matrix for C if and only if G is a parity check matrix of $C^\perp$. For basic results on codes we refer to [43].

Let F_q be a finite field. For a given k and q, let $G_k(q)$ be a $k \times (q^k - 1)/(q - 1)$ matrix over F_q in which any two columns are linearly independent. The code generated by the matrix $G_k(q)$ is called a **Simplex code** and is denoted by $S_k(q)$. $S_k(q)$ is a $[(q^k-1)/(q-1), k, q^{k-1}]$ q-ary code. Any code with these parameters is equivalent to Simplex code [19]. Thus $G_k(q)$ can be defined inductively by

$$G_2(q) = \begin{bmatrix} 0 & 1 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 1 & \alpha_3 & \cdots & \alpha_q \end{bmatrix}$$

and

$$(2.2) \quad G_k(q) = \left[\begin{array}{c|c|c|c|c|c} 0 \ \cdots \ 0 & 1 & 1 \ \cdots \ 1 & \alpha_3 \ \cdots \ \alpha_3 & \cdots & \alpha_q \ \cdots \ \alpha_q \\ \hline G_{k-1}(q) & \begin{matrix}0\\ \vdots \\ 0\end{matrix} & G_{k-1}(q) & G_{k-1}(q) & \cdots & G_{k-1}(q) \end{array}\right]$$

In $S_k(q)$ every nonzero codeword has weight q^{k-1}. The dual of the Simplex code is the well known $[(q^k-1)/(q-1),\ (q^k-1)/(q-1)-k,\ 3]$ q-ary **Hamming code.**

A nice way to construct a new code from a given code is by puncturing or appending one or more coordinates. For $1 \le u \le k-1$, let $G_{k,u}(q)$ be the matrix obtained from $G_k(q)$ by deleting columns corresponding to the columns of $G_u(q)$. That is,

$$G_{k,u}(q) = \left[G_k(q) \quad \backslash \quad \left[\begin{array}{c} 0 \\ \hline G_u(q) \end{array}\right] \right].$$

where 0 is a $(k-u)\times(q^u-1)/(q-1)$ zero matrix and $[A\backslash B]$ denotes the matrix obtained from the matrix A by deleting the columns of the matrix B. The code $C_{k,u}(q)$ generated by $G_{k,u}(q)$ is the punctured code of $S_k(q)$ and is called a **MacDonald code.** Binary case of it was first introduced by MacDonald [41]. However for $q \ge 3$, these codes were employed [49] to solve a classical combinatorial problem. $C_{k,u}(q)$ is a $[(q^k-q^u)/(q-1),\ k,\ q^{k-1}-q^{u-1}]$ q-ary linear code in which every non-zero codeword has weight either q^{k-1} or $q^{k-1} - q^{u-1}$.

Direct sum of two codes C_1 and C_2, denoted by $C_1 \oplus C_2$ is the code

$$C_1 \oplus C_2 = \{ (x,y) \mid x \in C_1 \text{ and } y \in C_2 \}.$$

If C_1 and C_2 are linear codes with generator matrices G_1 and G_2, respectively and dim $C_1 \geq$ dim C_2, then the code C generated by the matrix

$$G = \left[\begin{array}{c|c} G_1 & \begin{matrix} G_2 \\ 0 \end{matrix} \end{array} \right]$$

is called the **concatenation** of C_1 and C_2 .

For each i, let A_i and B_i be the number of codewords of weight i in C and $C^{\perp}$, respectively. The sequence $\{A_i\}_{i=0}^{n}$ is called the **weight distribution** of C. In 1963, MacWilliams [42] has given a set of equations relating the weight distribution of a code C and $C^{\perp}$. These are called the **MacWilliams identities.** These can be put in the following form [50] .

$$(2.3) \qquad \sum_{j=0}^{n-t} \binom{n-j}{t} A_j = q^{k-t} \sum_{j=0}^{t} \binom{n-j}{n-t} B_j \quad \text{for } t = 0,\ 1,\ \ldots,\ n$$

2.1 OPTIMAL CODES.

For a given k and d, let $n_q(k, d) = \min\{ n \mid$ there exists an [n, k, d] q-ary code $\}$. In 1960, Griesmer [22] gave a lower bound for $n_2(k, d)$. Later Solomon and Stiffler [53] generalized it to the q-ary case and is given by

$$n_q(k, d) \geq \sum_{i=0}^{k-1} \lceil d/q^i \rceil \equiv g_q(k, d) \tag{2.4}$$

where $\lceil x \rceil$ denotes the least integer greater than or equal to x. The bound (2.4) is known as the **Griesmer bound.** The $[n_q(k,d),k,d]$ q-ary code is said to be an **optimal code**. A $[g_q(k,d), k, d]$ code, if it exists, is called a **code meeting the Griesmer bound.** Well known examples of codes that meet the Griesmer bound are the Simplex code and the MacDonald code. A large class of codes that meet the Griesmer bound are obtained by certain puncturing of concatenation of two or more copies of a Simplex code. Such codes are called of BV type [29]. A necessary and sufficient condition for the existence of a code of BV type is given by the following proposition

Proposition 2.1 [30]. For given q, k and d, write

$$d = sq^{k-1} - \sum_{i=1}^{p} q^{u_i - 1} ,$$

where $s = \lceil d/q^{k-1} \rceil$, $k > u_1 \geq u_2 \geq . . . \geq u_p \geq 1$, and atmost q-1 u_i's take any given value. Then there exists a $[g_q(k,d),k,d]$ code of type BV if and only if $\sum_{i=1}^{\min\{s+1,p\}} u_i \leq sk$.

A similar result was also obtained by Dodunekov [14]. The binary version of it was first proved by Belov [2] in 1972.

Determining $n_q(k,d)$ in general is a difficult task. In recent years, Baumert and McEliece [1], Tilborg [59], Dodunekov and Manev [16] and many others have worked on determining $n_2(k, d)$ for small values k. By Proposition 2.1, $n_2(k, d) = g_2(k, d)$ for k

iv) If $A_j > 0$, then $A_i = 0$ for $i > qn-(q-1)d - j$ and $i \neq j$.

If C is a binary [n,k,d] code which meets the Griesmer bound and if $d \leq 2^{k-1}$, then MacWilliams and Sloane [43] have shown that any generator matrix of C has no repeated columns, that is $B_2 = 0$. In 1992, Hill and Newton have given the following improvement that holds for q-ary codes.

Proposition 2.5 [30]. Suppose C is an [n, k, d] q-ary code which meets the Griesmer bound and suppose j is a positive integer such that $d \leq q^{k-j+1}$. Then $B_j = 0$.

An updated detailed information of bounds on $n_2(8, d)$ can be obtained from the table of Verhoeff [60]. It is observed that for $k \leq 8$ and $d > 2^{k-1}$, $n_2(k, d) = g_2(k,d)$. However this is not true for $k \geq 9$. In [40] Logachev has shown that a binary $[g_2(9,336), 9, 336]$ code does not exist.

It was shown independently by Hamada and Tamari [26] and Dodunekov [14] that the bound given by (2.4) is reached for any q-ary linear code of dimension 2. In recent years Hamada [23] in cooperation with Deza [24], Helleseth [25] and Tamari [26], have characterized many values of d for which $n_q(k,d) = g_q(k,d)$, $k \geq 3$ by relating the problem to that of characterizing min. Hypers in a finite projective geometry. The following three propositions summarize results on $n_q(k, d)$.

Proposition 2.6 [14]. If $3 \leq q \leq k$ and $2q^i < d \leq q^{i+1}$ for $0 \leq i \leq k - q$, then $n_q(k, d) > g_q(k, d)$.

Proposition 2.7 [14]. Let $q|d$. If $n_q(k, d) = g_q(k, d)$, then $n_q(k, d - a) = g_q(k, d - a)$ for all $1 \leq a \leq q - 1$. Conversely if

$n_q(k, d-a) > g_q(k, d-a)$ for some $1 \le a \le q - 1$, then $n_q(k,d-b) > g_q(k, d-b)$ for all $0 \le b \le a$.

Proposition 2.8 [14]. If q is even and $q \ge 4$, then $n_q(3, d) = g_q(3, d)$ for all $d \le q + 2$. If q is odd, then

$$n_q(3, d) = \begin{cases} g_q(3,d) & \text{for } d < q \text{ and } d = q + 1 \\ g_q(3,d) + 1 & \text{for } d = q. \end{cases}$$

In [30], Hill and Newton have determined $n_3(3,d)$, $n_3(4,d)$ for all d and $n_3(5,d)$, for all but 30 values of d. The values of $n_3(5,d)$ for remaining values of d have now all been found (by nine authors of 10 different papers) [64], [65], [66], [67] and [68]. Values of $n_4(4,d)$ for all d have been obtained by Bhandari and Garg [5] and Greenough and Hill [21].

For showing nonexistence of certain codes, Tilborg introduced the concept of binary residual code [59]. Dodunekov further extended it to q-ary codes.

Definition 2.1 [14]. Let G be a generator matrix of a linear [n, k, d] code C over F_q and let $c \in C$. Let G_1 be the matrix obtained from G by deleting those columns where c has a nonzero entry. The code generated by G_1 is called the **residual code** of C with respect to the codeword c and is denoted by Res(C,c).

If only weight w of c is relevant, we usually write Res(C,w) for Res(C,c). The following proposition describes the parameters of a residual code.

Proposition 2.9 [14]. Suppose C is an [n, k, d] code over GF(q) and let c be a codeword of weight w. If $d>w(q-1)/q$, then Res(C,c) is an $[n - w, k - 1, d_1]$ code where $d_1 \ge d - w + \lceil w/q \rceil$.

Using above proposition Bhandari and Garg have observed the following.

Proposition 2.10 [5]. If C is an [n, k, d] q-ary code having a vector of weight w, $w < d + \lceil w/q \rceil$, then $w \leq n - k + 1$.

For q = 4, they proved the following

Proposition 2.11 [5]. If $k \geq 4$ and $d \in \{ 4^{k-2} - 1, 4^{k-2}, 2.4^{k-2} - 5, 2.4^{k-2} - 4, 3.4^{k-2} - 5, 3.4^{k-2} - 4 \}$, then $n_4(k, d) > g_4(k, d)$.

2.2 The Covering Radius.

Let C be an (n, M, d) q-ary code. Then spheres of radius $\lfloor (d-1)/2 \rfloor$ around codewords are disjoint, but they need not cover the whole space F_q^n. The smallest integer R such that spheres of radius R around codewords cover the whole space is called the covering radius of the code and is denoted by R(C). Many equivalent criteria for the covering radius of linear codes are known [11]. For example, the covering radius of a linear code is:

1. the weight of a maximum weight coset leader
2. the least integer R such that any (n - k)-tuples over GF(q) (called **syndrome**) is a linear combination of some R or fewer columns of any parity check matrix of the code.

The covering radius is a basic geometric parameter of a code. It is a measure of the quality of a code C, that is, maximal codes are characterized by the condition $R(C) \leq d(C) - 1$. If the code C is used for data compression or source coding (redundancy in the encoder input sequence is reduced or removed) the covering radius is a measure of the maximum distortion; if for error correction, $R(C)$ is the maximum weight of a correctable random error.

Determining covering radius of a given code, in general, is difficult. One of the simple upper bounds on the covering radius of an $[n,k,d]$ q-ary code C is the **redundancy bound:**

$$R(C) \le n - k. \tag{2.6}$$

If ρ is the least positive integer for which

$$\sum_{i=0}^{\rho} \binom{n}{i} (q - 1)^i \ge q^{n-k}, \tag{2.7}$$

then $R(C) \ge \rho$. This bound is known as the **sphere covering bound.** Since spheres of radius $\lfloor (d-1)/2 \rfloor$ around codewords are disjoint, $R(C) \ge \lfloor (d-1)/2 \rfloor$. Here $\lfloor x \rfloor$ is the greatest integer which is less than or equal to x. If $R(C) = \lfloor (d-1)/2 \rfloor$, then the code C is called a **perfect code.**

A lower bound for the covering radius of an $[n, k]$ q-ary code is $t_q[n,k]$, the minimal covering radius of any $[n, k]$ code. This was first defined by Cohen, Karpovsky, Mattson and Schatz [11] for $q = 2$. Obviously $t_q[n,k] \ge \rho$, where ρ is given by (2.7). In [20], Graham and Sloane have given a table of bounds on $t_2[n,k]$ for $1 \le k \le n \le 64$. For certain n and k, Calderbank and Sloane [9] have determined the exact value of $t_2[n,k]$.

The following proposition describes the effect of puncturing or appending a code on its covering radius

Proposition 2.12 [11]. Appending an overall parity check or the zero parity check to the generator matrix of a given code increases the covering radius by one. On the other hand puncturing a code on p coordinates reduces the covering radius by atmost p.

Above proposition is also true for non-linear codes.

If C_0 and C_1 are binary codes generated by matrices G_0 and G_1, respectively and if C is the code generated by the matrix

$$G = \left[\begin{array}{c|c} 0 & G_1 \\ \hline G_0 & A \end{array}\right],$$

then Mattson [45] has shown that

$$R(C) \le R(C_0) + R(C_1) \tag{2.8}$$

and the covering radius of D, concatenation of C_0 and C_1 satisfy the following inequality

$$R(D) \ge R(C_0) + R(C_1) \tag{2.9}$$

The inequalities (2.8) and (2.9) also hold for q-ary codes, the proof is similar to that for binary codes.

The best known upper bound on the covering radius of an [n,k,d] code is given by Janwa [35].

Proposition 2.13 [35]. Let C be an [n, k, d] code, then
$$R(C) \le n - \sum_{i=1}^{k} \lceil d/q^i \rceil \equiv H_q(n, k, d).$$

If the code meets the Griesmer bound, then $R(C) \le d - \lceil d/q^k \rceil$. For binary codes this inequality was first proved by Busschbach, Gerretzen and Tilborg [7]. Later this was extended by Janwa [35] to any optimal code. Using this bound, Janwa showed that the covering radius of the q-ary repetition code of length n is atmost $\lfloor n(q-1)/q \rfloor$. The following Lemma shows that we have the equality.

Lemma 2.1. The covering radius of an [n,1,n] q-ary repetition code C is $\lfloor n(q-1)/q \rfloor$.

Proof. Let $C = \{ \bar{\alpha} \mid \alpha \in F_q \}$, where $\bar{\alpha} = (\alpha, \alpha, \cdots, \alpha)$, $t = \lceil n/q \rceil$ and let

$$x = \overbrace{0\ 0 \cdots 0}^{t}\ \overbrace{1\ 1 \cdots 1}^{t}\ \overbrace{\alpha_3\ \alpha_3 \cdots \alpha_3}^{t} \cdots \overbrace{\alpha_{q-1} \cdots \alpha_{q-1}}^{t}\ \overbrace{\alpha_q\ \alpha_q \cdots \alpha_q}^{n-(q-1)t}$$

Then $d(x,C) = \min\{ n - \lceil n/q \rceil, (q-1)\lceil n/q \rceil \} = n - \lceil n/q \rceil$. So $R(C) \geq \lfloor n(q-1)/q \rfloor$.■

Using Proposition 2.13, Janwa proved that covering radius of a k-dimensional q-ary Simplex code $S_q(q)$ is less than or equal to $q^{k-1} - 1$. The same bound have been given independently by Dodunekov [14] and Garg [19].

Let $b_q(k, d) = n_q(k+1, d) - n_q(k, d)$. In [19] Garg has given the following better upper bound for the covering radius of an optimal code.

Proposition 2.14 [19]. The covering radius of an $[n_q(k, d), k, d]$ code is atmost $d - b_q(k, d)$. Moreover if $b_q(k, d) = 1$, then there is an $[n_q(k, d), k, d]$ code with covering radius $d - 1$.

By making use of above proposition, Garg has determined the exact covering radius of a 2-dimensional q-ary Simplex code for q even and an upper bound for q odd.

Proposition 2.15 [19]. i) If q is even, then $R(S_2(q)) = q - 1$.

ii) If q is odd, then $R(S_2(q)) \le q - 2$.

Let $t_k(q)$ be the maximum number of (-1)'s in any codeword of $S_k(q)$ and let $\underline{1}$ denotes the all one vector of length $n = (q^k-1)/(q-1)$. Then $w(\underline{1}+S_k(q))$, the weight of the coset leader in $\underline{1} + S_k(q)$ is $n - t_k(q)$ and hence $R(S_k(q)) \ge n - t_k(q)$ [19]. If for some positive integer k_0 there exists a vector $a = (a_1,a_2,\cdots,a_n) \in S_{k_0}(q)$ of weight n with $w(a+S_{k_0}(q)) = R(S_{k_0}(q))$, then Garg [19] has shown that

$$R(S_k(q)) \ge n - q^{k-k_0} t'_{k_0}(q) \tag{2.10}$$

for all $k \ge k_0$ where $t'_{k_0}(q)$ is the maximum number of (-1)'s in any codeword of a code equivalent to $S_{k_0}(q)$. Using (2.10) and Proposition 2.14, Garg obtained the following bounds for $R(S_k(3))$, $R(S_k(4))$ and $R(S_k(5))$.

Proposition 2.16 [19].

i) $3^{k-1} - (3^{k-2} + 1)/2 \le R(S_k(3)) \le 3^{k-1} - 2$ for $k \ge 3$.

ii) $4^{k-1} - (2.4^{k-2} + 1)/3 \le R(S_k(4)) \le 4^{k-1} - 2$ for $k \ge 3$.

iii) $R(S_k(5)) \ge (3.5^{k-1} - 2.5^{k-2} - 1)/4$

For binary codes that meet the Griesmer bound, Garg has given the following lower bound on its covering radius.

Proposition 2.17 [19]. If C is a binary $[g_2(k,d), k, d]$ code with $d \le 2^{k-1}$, then $R(C) \ge g_2(k,d) - 2^{k-1}$.

2.3 THE COVERING CODES.

Let C be a (q, n, M)R code of length n with M codewords and covering radius R over F_q . Let $K_q(n, R) = \min \{ M \mid$ there is a (q, n, M)R code $\}$. The general problem of determining the values of the function $K_q(n, R)$ is known as the **covering problem**. For q = 3 and R = 1, this problem is popularly known as the **'football pool problem'**.

Determining $K_q(n,R)$ in general is difficult. One of the simple lower bound on $K_q(n, R)$, is the well known sphere covering bound

$$(2.11) \qquad K_q(n, R) \geq q^n / \sum_{i=0}^{R} \binom{n}{i} (q - 1)^i$$

In most cases, the sphere covering bound seems to be far from accurate. Therefore, finding significant improvements on the sphere covering bound has turned out to be a challenging problem. In [31], Honkala and in [61], van Wee have independently determined better lower bounds on $K_q(n,R)$ by using the concept of Excess on a subset of the whole space by the code C.

In recent years researchers have improved the upper bound on $K_q(n, R)$ by constructing good covering codes. Quite often the amalgamated direct sum of two codes that have certain partitioning properties is a good covering code. Normal and subnormal codes are examples of such codes [39]. Binary versions of these codes were introduced by Graham et al [20] and Honkala [31].

Definition 2.2. [39]. Let C be a (q,n,M)R code. For i = 1, 2,⋯, n and $\alpha \in F_q$, let $C_\alpha^{(i)} = \{ (c_1,c_2, \cdots , c_n) \in C \mid c_i = \alpha \}$ and

$$N^{(i)} = \max_{x \in F_q^n} \{ \sum_{\alpha \in F_q} d(x, C_\alpha^{(i)}) \}$$

with the convention that $d(x, \phi) = n$; $N^{(i)}$ is called the norm of C with respect to coordinate i. If for some i, $N^{(i)} \le qR + q - 1$, then C is said to be **normal**, and the coordinate i is called **acceptable.**

In 1991, Honkala [32] has introduced the concept of a (k,t)-subnormal covering code .

Definition 2.3 [32]. A (q, n, M)R code C has (k,t)-**subnorm** S if there is a partition $\{C_i\}_{i=1}^k$ of C such that for all x with $R - t \le d(x, C) \le R$,

$$\min_i \{ d(x,C_i) \} + \max_i \{ d(x,C_i) \} \le S$$

Such a partition is called **acceptable**. If S = 2R + 1, then C is called (k,t)-**subnormal**.

Using this concept, he proved the following.

Proposition 2.18 [32]. If there is a (q,q-2)-subnormal (q,n,M)R code, then there exists a (q,n+q,M)R+q-1 code.

In 1991, Ostergard introduced the concepts of seminormal and strongly seminormal codes to get further improvements on upper bounds for $K_q(n,R)$.

Definition 2.4 [47]. A (q, n, M)R code C is said to be **seminormal** if there exists a partition of C into q subsets C_α , $\alpha \in F_q$ such that for all $x \in F_q^n$, with $d(x, C) = R$,

$$\max_{\alpha \in F_q} \{ d(x, C_\alpha) \} \le R + 1. \tag{2.12}$$

If (2.12) is true for all $x \in F_q^n$, then C is said to be **strongly seminormal**. The partition $\{ C_\alpha \}_{\alpha\in F_q}$ is called **acceptable.**

Let A be a $(q, n_1, M_1)R_1$ code and let B be a $(q, n_2, M_2)R_2$ strongly seminormal code with an acceptable partition $\{B_\alpha\}_{\alpha\in F_q}$. For each $\alpha \in F_q$, let $A_\alpha = \{ c \mid (c,\alpha) \in A \}$. If $A_\alpha \ne \phi$ for all $\alpha \in F_q$ let $C_\alpha = \{ (u,v) \mid u \in A_\alpha , v \in B_\alpha \}$. Then $C = \bigcup_{\alpha\in F_q} C_\alpha$ is called an **amalgamated direct sum (ADS)** of A and B with parameters $(q, n_1+n_2-1, \sum_{\alpha\in F_q} |A_\alpha||B_\alpha|)$ and is denoted by $A \dot{\oplus} B$.

The above definition of ADS generalizes the original definition of [12] to the case where one code is partitioned not by values of codewords at a coordinate place but arbitrarily into q cells.

Since $\bigcup_{\alpha\in F_q} A_\alpha$ is the punctured code of A, $R(A\dot{\oplus}B) \ge R_1 + R_2 - 1$.

The following proposition of Ostergard gives an upper bound for the covering radius of $A\dot{\oplus}B$ in case B is strongly seminormal.

Proposition 2.19 [47]. Let A be a $(q, n_1, M_1)R_1$ code with $A_\alpha = \{ c \mid (c,\alpha) \in A \} \ne \varnothing$ for all $\alpha \in F_q$. If B is a $(q, n_2 , M_2)R_2$

trongly seminormal code with $\{B_\alpha\}_{\alpha \in F_q}$ an acceptable partition, hen the covering radius of $A\dot{\oplus}B$ is at most $R_1 + R_2$.

The following proposition of Ostergard gives an upper bound ɔ $K_q(n,R)$.

<u>**roposition 2.20 [47].**</u> For $0 \le p \le q - 2$, $K_q(qr-p,\ qr-r-p-1) \le$ (p+2).

For linear codes, finding $K_q(n,\ R)$ is same as determining ıe minimum dimension k such that an [n, k] code with covering adius R exist. This problem is equivalent to the problem of etermining $l(m,R;q)$, the minimum length n such that an $[n,\ n-m]R$ -ary code exists. This function was first introduced by Brualdi, Less and Wilson [6]. They showed that $l(km,\ r;\ q) \le$ $(q^k-1)/(q-1).l(m,\ r;\ q^k)$ and gave a table of bounds for $l(m,r;2)$ .th $1 \le r \le n \le 12$. Struik [57] and Calderbank and Sloane [9] ıve given bounds on $l(m,r;2)$. Almost nothing is known about ary case.

Let $q_1, q_2, \cdots, q_m$ and $n_1, n_2, \cdots, n_m$ be given. Let $n =$ $+ n_2 + \cdots + n_m$ and let $H = \{ u = (u_1, u_2, \cdots, u_m) \mid u_i \in F_{q_i}^{n_i},\ i$ $1,\ 2,\ \cdots,\ m\}$. Since each u_i is an n_i-tuple, u is an n-tuple. m ≥ 2 and if there are indices $i,\ j \le m$ such that $q_i \ne q_j$, the ›ace called a proper mixed space and a nonempty subset C of is d a **mixed code**. A mixed code C with covering radius R $(q_1,\ q_2, \cdots,\ q_m;\ n_1,\ n_2, \cdots,\ n_m;\ M)R$ code. Further, $_m(n_1, n_2, \cdots, n_m; R) = \min\{\ M \mid$ there is a

:rongly seminormal code with $\{B_\alpha\}_{\alpha\in F_q}$ an acceptable partition, ıen the covering radius of $A\dot{\oplus}B$ is at most R_1+R_2.

The following proposition of Ostergard gives an upper bound › $K_q(n,R)$.

·oposition 2.20 [47]. For $0 \le p \le q-2$, $K_q(qr-p, qr-r-p-1) \le$ p+2).

For linear codes, finding $K_q(n, R)$ is same as determining .e minimum dimension k such that an [n, k] code with covering .dius R exist. This problem is equivalent to the problem of termining $l(m,R;q)$, the minimum length n such that an $[n, n-m]R$ ary code exists. This function was first introduced by Brualdi, ess and Wilson [6]. They showed that $l(km, r; q) \le$ $^k-1)/(q-1).l(m, r; q^k)$ and gave a table of bounds for $l(m,r;2)$ th $1 \le r \le n \le 12$. Struik [57] and Calderbank and Sloane [9] ve given bounds on $l(m,r;2)$. Almost nothing is known about ary case.

Let $q_1, q_2, \cdots, q_m$ and $n_1, n_2, \cdots, n_m$ be given. Let $n =$ $+ n_2 + \cdots + n_m$ and let $H = \{ u = (u_1,u_2,\cdots,u_m) \mid u_i \in F_{q_i}^{n_i}, i$ $1, 2, \cdots, m\}$. Since each u_i is an n_i-tuple, u is an n-tuple. $m \ge 2$ and if there are indices $i, j \le m$ such that $q_i \ne q_j$, the ace H is called a proper mixed space and a nonempty subset C of is called a **mixed code**. A mixed code C with covering radius R called a $(q_1, q_2,\cdots, q_m; n_1, n_2,\cdots, n_m; M)R$ code. Further, $_{1},q_2,\cdots,q_m(n_1,n_2,\cdots,n_m;R) = \min\{ M \mid$ there is a

$(q_1, q_2, \cdots, q_m; n_1, n_2, \cdots, n_m; M)R$ code $\}$. The upper and lower bounds on mixed covering codes have been studied in [27, 38, 48, 52]. If $q_1 = q_2 = \cdots = q_m = q$, then the code is a $(q, n, M)R$ code.

Chapter III

Covering Codes

In [47] Ostergard conjectured the existence of (5, 6, 25)3 and (5, 6, 125)2 strongly seminormal codes. In this Chapter, we construct a family of strongly seminormal and some other strongly seminormal codes that including the above codes. Better lower and upper bounds on $K_q(n,R)$ are also obtained. These give many improvements in the tables of [47]. Throughout this Chapter $F_q = \{ \alpha_1 = 0,\ \alpha_2 = 1,\ \alpha_3\ ,\ \cdots\ ,\ \alpha_q \}$.

3·1 STRONGLY SEMINORMAL CODES·

Let q be a prime power and let $S_2(q)$ be the 2-dimensional q-ary Simplex code. Let A be a [q, 2, q - 1] q-ary linear code generated by the matrix

$$G_A = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \alpha_3 & \cdots & \alpha_q \end{bmatrix} \tag{3.1}$$

Then A is a punctured code of $S_2(q)$.

Theorem 3.1. The covering radius of A is q - 2.

Proof. By Proposition 2.8, $n_q(3, q-1) = q + 1$ and hence $b_q(2,q-1) = 1$. Therefore by Proposition 2.14, there exists a [q, 2, q - 1] code C with covering radius q - 2. Since the code C meets the Griesmer bound, $B_1 = 0$. The MacWilliams identities (2.3) for B_0 and B_1 give

$$A_{q-1} + A_q = q^2 - 1$$
$$A_{q-1} + A_q = q(q-1)$$

Solving these equations one gets $A_{q-1} = q(q - 1)$ and $A_q = q - 1$. Without loss of generality it can be assumed that C has a generator matrix G whose first row is the all one vector. Since the minimum distance of C is q - 1, the second row of G must have distinct coordinates. Therefore G is equivalent to the matrix G_A. Since equivalent codes have same covering radius, R(A) = q - 2.■

Let A be the [q+1, 2, q-1]q-2 code defined above. Then there exists $y = (y_1, y_2, \cdots, y_q) \in F_q^q$ such that d(y, A) = q - 2. So $S = \{ c \in A \mid d(y, c) = q - 2 \} \neq \phi$. Let C be the [q, 3, q-2] MDS code generated by the matrix $\begin{bmatrix} G_A \\ y \end{bmatrix}$. The MacWilliams identities (2.3) give $A_{q-2} = (q-1)q(q-1)/2$. Hence $|S| = q(q-1)/2$. Therefore for any two coordinate positions i and j, there exists $c \in S$ such that $c_i = y_i$ and $c_j = y_j$. Since the strength of the code A is two, that is, any two coordinate positions of A have all ordered pairs appearing equal number of times, such a c is unique and is denoted by c(i,j).

Let $A_\alpha^{(1)} = \{ c = (c_1, c_2, \cdots, c_q) \in A \mid c_1 = \alpha \}$. For convenience, we can write the elements of $A_\alpha^{(1)}$ as a qxq array

$$A_\alpha^{(1)} = \left[\begin{array}{c|ccc} \alpha & \alpha & \cdots & \alpha \\ \hline \alpha & & & \\ \vdots & & B_\alpha & \\ \alpha & & & \end{array}\right] \qquad (3.2)$$

It is observed that every codeword of A that is not a multiple of all one vector has distinct coordinates. Hence every row and column of B_α has distinct entries. For each $i \in \{1, 2, \cdots, q-1\}$, let $A_{y_i} = \{ c(i,j) \mid i < j \le q \}$, then $|A_{y_i}| = q - i$, $S = \bigcup_{i=1}^{q-1} A_{y_i}$ and $A_{y_1} \le A_{y_1}^{(1)}$.

Using the above said notations, we prove the following two Lemmas.

Lemma 3.1. If i, j and m are distinct positive integers, then

i) $A_{y_i} \cap A_{y_j} = \phi$, ii) $A_{y_i} \cap A_{y_1}^{(1)} = \phi$ for $i > 1$.

iii) $|A_{y_i} \cap A_\alpha^{(1)}| = 0$ or 1 for $\alpha \in F_q \backslash \{ y_1 \}$.

iv) For $i > 1$, if $c(i,j) \in A_\alpha^{(1)} \cap S$, then $c(i,m)$, $c(m,i)$, $c(m,j)$, $c(j,m) \notin A_\alpha^{(1)} \cap S$.

Proof. i) Suppose $c \in A_{y_i} \cap A_{y_j}$. Then there exist integers $r > i$ and $s > j$ with $c_k = y_k$ for $k = i, j, r$ and s. Therefore $d(c, y) \le q - 3$ and hence $c \notin S = \bigcup_{i=1}^{q-1} A_{y_i}$, a contradiction. Thus $A_{y_i} \cap A_{y_j} = \phi$ for $i \ne j$.

ii) If $c \in A_{y_i} \cap A_{y_1}^{(1)}$ for some $i > 1$, then there is an integer $j > i$ such that $c_k = y_k$ for $k = i$ and j. Since $c \in A_{y_1}^{(1)}$, $d(c, y) \le$

$q - 3$, a contradiction. Hence $A_{y_i} \cap A_{y_1}^{(1)} = \phi$ for $i > 1$.

iii) If $i = 1$, then $A_{y_1} \cap A_\alpha^{(1)} = \emptyset$ for $\alpha \neq y_1$ as $A_{y_1} \subseteq A_{y_1}^{(1)}$. Suppose $|A_{y_i} \cap A_\alpha^{(1)}| \geq 2$ for some $i > 1$ and $\alpha \in F_q \backslash \{y_1\}$. Without loss of generality, let $|A_{y_i} \cap A_\alpha^{(1)}| = 2$ and let $u, v \in A_{y_i} \cap A_\alpha^{(1)}$. Then there exist integers $r > i$ and $s > i$ with $u_k = y_k$ for $k = i$, r, $v_m = y_m$ for $m = i, s$. Therefore y_i appears twice in the $(i-1)$th column of B_α, where B_α is defined by (3.2), a contradiction. Hence $|A_{y_i} \cap A_\alpha^{(1)}| = 0$ or 1 for all i and $\alpha \neq y_1$.

iv) Let $c = c(i,j) \in A_\alpha^{(1)} \cap S$. If $u = c(i,m) \in A_\alpha^{(1)} \cap S$, then $u_i = y_i$ and $u_m = y_m$. Therefore $d(c,u) \leq q - 2$. Since minimum distance of A is $q - 1$, $c = u$ and hence $d(c, y) \leq q - 3$. So $c \notin S$, a contradiction. Hence $c(i,m) \notin A_\alpha^{(1)} \cap S$. Similarly $c(m,i)$, $c(j,m)$ and $c(m,j) \notin A_\alpha^{(1)} \cap S$.

<u>**Lemma 3.2.**</u> If q be even and $d(y, A) = q - 2$, then $d(y, A_\alpha^{(1)}) = q-2$ for all $\alpha \in F_q$.

<u>**Proof.**</u> Let $\alpha \in F_q$ and let $y \in F_q^q$ with $d(y, A) = q - 2$. Since $A_{y_1} \subseteq A_{y_1}^{(1)}$, $S \cap A_{y_1}^{(1)} \neq \phi$. Therefore $d(y, A_{y_1}^{(1)}) = q - 2$. Let $S_1 = S \backslash A_{y_1}$, then $|S_1| = (q-1)(q-2)/2$. If $c(i,j) \in S_1 \cap A_\alpha^{(1)}$ for some i and j, then by Lemma 3.1 (iv), $c(i,m)$, $c(m,i)$, $c(j,m)$ and $c(m,j)$ $\notin S_1 \cap A_\alpha^{(1)}$ for all m distinct from i and j. Hence $|S_1 \cap A_\alpha^{(1)}| \leq (q-1)/2$. Since q is even, $|S_1 \cap A_\alpha^{(1)}| \leq (q-2)/2$. So S_1 intersects $A_\beta^{(1)}$ nontrivially for at least $q - 1$ distinct β's, different from y_1 and hence $d(y, A_\beta^{(1)}) = q - 2$. for all $\beta \neq y_1$. ■

Let $A_\alpha^{(1)}$ be as defined by (3.2) above and let $C = \bigcup_{\alpha \in F_q} C_\alpha$, where $C_\alpha = \{ (\alpha,c) \mid c \in A_\alpha^{(1)} \}$. Then C is a [q+1, 2, q - 1] q-ary linear code generated by the matrix

$$(3.3) \qquad G = \begin{bmatrix} 1 & 1 & 1 & 1 & . & . & . & 1 \\ 0 & 0 & 1 & \alpha_3 & . & . & . & \alpha_q \end{bmatrix}$$

Its covering radius is given by the following theorem.

Theorem 3.2. Let q be even and let C be the code defined above, then $R(C) = q - 2$.

Proof. Let A be the code generated by the matrix (3.1) and let $x \in F_q^{q+1}$. Then $x = (\alpha, y)$, $\alpha \in F_q$ and $y \in F_q^q$. By Theorem 3.1, $d(y,A) \leq q - 2$. If $d(y,A) \leq q - 3$, then $d(x,C) \leq q - 2$. If $d(y,A) = q - 2$, then by Lemma 3.2, $d(y, A_\beta^{(1)}) = q - 2$ for all $\beta \in F_q$. Therefore $d(x, C_\alpha) = q - 2$ and $d(x, C_\beta) = q - 1$ for $\beta \neq \alpha$. Hence $R(C) = q - 2$.■

Theorem 3.3. Let C be the code generated by the matrix G in (3.3). If q is odd, then $R(C) = q - 2$ for $q \geq 7$.

Proof. Let q be odd. By (2.6), $R(C) \leq q - 1$. Since G does not contain a zero column, $B_1 = 0$. The MacWilliams identities (2.3) give

$$\begin{aligned} A_{q-1} + A_q + A_{q+1} &= q^2 - 1 \\ 2A_{q-1} + A_q + \phantom{A_{q+1}} &= (q+1)(q-1) \end{aligned}$$

Therefore $A_{q-1} = A_{q+1} = q - 1$. Hence the weight distribution of C is:

$$A_0 = 1,\ A_{q-1} = q - 1,\ A_q = (q-1)^2 \text{ and } A_{q+1} = q - 1.$$

If $R(C) = q - 1$, then there is a $x \in F_q^{q+1}$ such that $d(x,C) = q-1$. Since C is a linear code, we can choose x of weight $q - 1$. The matrix

$$G_D = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 1 & \alpha_3 & \cdots & \alpha_q \\ x_1 & x_2 & x_3 & & \cdots & x_{q+1} \end{bmatrix} = \begin{bmatrix} u \\ v \\ x \end{bmatrix}$$

generates a $[q+1, 3, q-1]$ code D. Let $\{A_i'\}$ and $\{B_i'\}$ be the weight distributions of D and $D^{\perp}$, respectively. Since D meets the Griesmer bound, by Proposition 2.5, $B_i' = 0$ for $i = 1, 2, 3$. The MacWilliams identities (2.3) for B_i' for $1 \le i \le 3$ give

$$\begin{aligned} A_{q-1}' + A_q' + A_{q+1}' &= q^3 - 1 \\ 2A_{q-1}' + A_q' &= (q+1)(q^2-1) \\ A_{q-1}' &= (q-1)q(q+1)/2 \end{aligned}$$

Solving these equations, one gets

$$A_0' = 1,\ A_{q-1}' = q(q^2 - 1)/2,\ A_q' = q^2 - 1 \text{ and } A_{q+1}' = (q - 1)^2 q/2.$$

Let $y_i = \alpha_i u + v$, $1 \le i \le q$, and $y_{q+1} = u$, then clearly no y_i is a scalar multiple of the others. Since $C = \bigcup_{\alpha \in F_q} \{\alpha y_i\}_{i=1}^{q+1}$ and each coordinate position of C has all elements from F_q appearing equal number of times, no two y_i's have zero in the same coordinate place. Since $w(x) = q - 1$, there exist two coordinates of x, say x_l and x_m are zero. So there exist y_r and y_s such that $y_{rl} = 0$ and $y_{sm} = 0$ where $y_r = (y_{r1}, y_{r2}, \cdots, y_{rq+1})$. If $y_{sl} = 0$, then the code obtained by puncturing lth and mth coordinates of the code generated by y_r and x is a $[q-1, 2, q-1]$ code but such a code does not exist. Therefore there is no y_i whose lth and mth coordinates are zero.

Let D_i be a $[q + 1, 2, q - 1]$ code generated by y_i and x. Let $\{A_j^{(i)}\}$ and $\{B_j^{(i)}\}$ be the weight distribution of D_i and $D_i^{\perp}$, respectively. If $i \in \{ r, s \}$, then D_i has exactly one zero coordinate identically zero. So the code D_i' obtained from D_i by puncturing this coordinate is a $[q, 2, q - 1]$ code. Then the MacWilliams identities (2.3) give

$$\begin{aligned} A_{q-1}^{(i)} + A_q^{(i)} &= q^2 - 1 \\ A_{q-1}^{(i)} &= q(q-1) \end{aligned}$$

Therefore the weight distribution of D_i is:

$$A_0^{(i)} = 1,\ A_{q-1}^{(i)} = q(q - 1),\ A_q^{(i)} = q - 1 \text{ and } A_{q+1}^{(i)} = 0.$$

If $i \notin \{ r, s \}$, then the MacWilliams identities (2.3) give

$$\begin{aligned} A_{q-1}^{(i)} + A_q^{(i)} + A_{q+1}^{(i)} &= q^2 - 1 \\ 2A_{q-1}^{(i)} + A_q^{(i)} &= (q-1)(q+1) \end{aligned}$$

By solving the above system of equations, we get

$$A_0^{(i)} = 1,\ A_{q-1}^{(i)} = A_{q+1}^{(i)}, \text{ and } A_q^{(i)} = q^2 - 1 - 2A_{q-1}^{(i)}.$$

If $i \in \{ 2, 3, \cdots, q \}$, then $A_q^{(i)} \neq 0$, say $A_q^{(i)} = (q-1)t$, $t \geq 1$. If $i \in \{r, s\}$, then from above $A_q^{(i)} = q-1$.

If $q \geq 5$, then there is an $i \notin \{ 1, r, s, q+1\}$ such that $A_q^{(i)} = (q - 1)t$, $t \geq 1$ and $A_{q-1}^{(i)} = A_{q+1}^{(i)}$. For this particular i, if

$A_q^{(i)} = q - 1$, then $A_{q-1}^{(i)} = A_{q+1}^{(i)} = q(q-1)/2$. Since $A_j^{(i)}$ is multiple of $q - 1$, $q/2$ must be an integer but q is odd. Therefore $A_q^{(i)} \geq 2(q - 1)$ for $i \notin \{ 1, r, s, q+1 \}$. Since the number of q weight vectors of D is a sum of number of q weight vectors of D_i's,

$$\begin{aligned} q^2 - 1 &= \sum_{\substack{i=2 \\ i\notin\{r,s\}}}^{q} A_q^{(i)} + A_q^{(1)} + A_q^{(r)} + A_q^{(s)} + A_q^{(q+1)} \\ &\geq (q + 1 - 4)2(q - 1) +0+ (q - 1) + (q - 1)+ 0 \\ &= 2(q - 3)(q - 1) + 2(q - 1) \\ &= 2(q - 2)(q - 1) \end{aligned}$$

which is not true for $q \geq 6$.∎

The code defined in the matrix G in (3.3) is in fact strongly seminormal. To see this we first make few observations.

<u>**Remark 3.1.**</u> If C is a $(q, n, M)R$ code and if $x \in F_q^n$, then $x + C$ is also a $(q, n, M)R$ code.

<u>**Remark 3.2.**</u> Let A be any $(q,n,M)R+1$ linear code and let $x \in F_q^n$. Define $C = \bigcup_{\alpha \in F_q} C_\alpha$, where $C_\alpha = \alpha x + A$. If the covering radius of C is atleast R, then C is a strongly seminormal code with $\{C_\alpha\}_{\alpha\in F_q}$ an acceptable partition.

<u>**Lemma 3.3.**</u> If C is a $(q,n,M)R$ strongly seminormal code, then $M \geq qK_q(n, R+1)$.

<u>**Proof.**</u> If C is a $(q, n, M)R$ strongly seminormal code with an acceptable partition $\{C_\alpha\}_{\alpha\in F_q}$, then $R(C_\alpha) \leq R + 1$ and hence $|C_\alpha| \geq K_q(n,R+1)$ for all $\alpha \in F_q$. Therefore $M \geq qK_q(n, R+1)$.∎

Let C_0 be the $[q + 1, 1, q + 1]q-1$ q-ary repetition code and let $C_\alpha = \alpha(0,0,1,\alpha_3,\cdots,\alpha_q) + C_0$, for $\alpha \in F_q$. By Remark 2.1, $R(C_\alpha)=q-1$ for all $\alpha \in F_q$. The code $C = \bigcup_{\alpha \in F_q} C_\alpha$ is a $[q+1,2,q-1]$ q-ary linear code. Moreover C is equivalent to the code generated by the matrix G in (3.3) and hence by Theorems 3.2 and 3.3, $R(C) = q - 2$ for all $q \geq 7$ and $q = 4$. By Remark 3.2 the following theorem follows.

<u>**Theorem 3.4.**</u> If $q \geq 7$ or $q = 4$, then the code generated by the matrix G in (3.3) is a $[q+1, 2, q-1]$ q-ary strongly seminormal linear code with covering radius q-2.

The following Example shows that the Theorem 3.4 is also true for $q = 5$.

<u>**Example 3.1.**</u> Let C be a [6, 2, 4] linear code over $\mathbb{Z}_5$ generated by the matrix

$$G = \begin{bmatrix} 3 & 0 & 1 & 2 & 3 & 4 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

and let C_0 be the repetition code of length 6. For each $\alpha \in \mathbb{Z}_5$, let $C_\alpha = \alpha(3,0,1,2,3,4) + C_0$. By Remark 3.1, $R(C_\alpha) = 4$ for all $\alpha \in \mathbb{Z}_5$. It is easily seen by computer that $R(C) = 3$. Hence, by Remark 3.2, C is a (5, 6, 25)3 strongly seminormal code with $\{C_\alpha\}_{\alpha\in\mathbb{Z}_5}$ an acceptable partition.

Since $K_q(q+1, q-1) = q$, by Lemma 3.3, cardinality of a q-ary strongly seminormal code of length $q + 1$ and covering radius $q - 2$ must be greater than or equal to q^2. Therefore C, the strongly seminormal code given by both the Theorem 3.4 and the Example above are of minimum cardinality. The code generated by the matrix G in (3.3) is strongly seminormal for $q = 3$ also. But its covering radius is 2.

Example 3.2. Let C be a [4, 2, 2] ternary code generated by the matrix

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 2 \end{bmatrix}.$$

If $x = (1,2,1,2)$, then $d(x, C) = 2$. Therefore by redundancy bound $R(C) = 2$. Let C_0 be the repetition code of length 4. For each $\alpha \in F_3$, let $C_\alpha = \alpha(0,0,1,2) + C_0$. Then C_α is a (3, 4, 9) code. Since $R(C_0) = 2$, by Remark 3.1, $R(C_\alpha) = 2$. Hence by Remark 3.2, C is a strongly seminormal with $\{C_\alpha\}_{\alpha \in F_q}$ an acceptable partition.

Example 3.3. Let C_0 be the code generated by G in Example 3.1, $x = (1, 0, 1, 3, 4, 0)$ and let C be a [6,3,3] 5-ary code generated by the matrix

$$G_C = \begin{bmatrix} G \\ x \end{bmatrix}.$$

For each $\alpha \in \mathbb{Z}_5$, let $C_\alpha = \alpha x + C_0$. Then $C = \bigcup_{\alpha \in \mathbb{Z}_5} C_\alpha$. It is easy to verify by computer that $R(C) = 2$. By Remark 3.1, C_α is a (5,6,25)3 code and hence by Remark 3.2, C is strongly seminormal with $\{C_\alpha\}_{\alpha \in \mathbb{Z}_5}$ an acceptable partition.

Example 3.4. Let C be a [11, 3, 6] ternary linear code with generator matrix

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 2 & 1 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 \end{bmatrix}$$

Using computer, it is seen that $R(C) = 5$. The code D generated by the first two rows of G is a $[11, 2, 7]6$ ternary linear code. For each $\alpha \in \mathbb{Z}_3$, let $C_\alpha = \alpha y + D$, where y is the last row G. By Remark 3.1, C_α is a $(3,11,9)6$ code and hence by Remark 3.2, C is a strongly seminormal code with $\{C_\alpha\}_{\alpha\in\mathbb{Z}_3}$ an acceptable partition.

It is observed that the cardinality of the codes given by Theorem 3.4, Examples 3.1, 3.3 and 3.4 are same as the upper bounds for $K_q(n, R)$ given by Ostergard [47]. But they are in addition strongly seminormal. These codes are used later to improve previous known upper bounds. A necessary and sufficient conditions for an optimal code to be strongly seminormal is given by the following theorem.

Theorem 3.5. Let C be an $[n=n_q(k,d), k, d]$ code. The code C is a strongly seminormal if and only if $R(C) = d - 1$.

Proof. Suppose $R(C) = d - 1$. For each $\alpha \in F_q$, let $C_\alpha^{(i)} = \{ c=(c_1,c_2, \cdots c_n) \in C \mid c_i = \alpha \}$, $1 \le i \le n$. Since C is an optimal code, $C_\alpha^{(i)} \ne \phi$ and $d(c, C_\alpha^{(i)}) \ge d$ for all $c \in C\backslash C_\alpha^{(i)}$. Therefore by Remark 3.1, $R(C_\alpha^{(i)}) \ge d$. If $R(C_0^{(i)}) \ge d + 1$, then there exists $x \in F_q^n$ such that $d(x, C_0^{(i)}) = d + 1$ and hence the code obtained by puncturing the ith coordinate of the code generated by x and $C_0^{(i)}$ is an $[n - 1, k, d]$ q-ary linear code, a contradiction. Therefore $R(C_0^{(i)}) = d$. By Remark 3.1, $R(C_\alpha^{(i)}) = d$ for all $\alpha \in F_q$ and hence by Remark 3.2, C is a strongly seminormal code with $\{C_\alpha^{(i)}\}_{\alpha\in F_q}$ an acceptable partition.

Conversely, let C be a strongly seminormal optimal code. Let $\{C_\alpha\}_{\alpha\in F_q}$ be a partition of C such that $R(C_\alpha) \le R(C) + 1$ for all $\alpha \in F_q$. For any $c \in C \backslash C_\alpha$, $d(c, C_\alpha) \ge d$. Therefore $R(C_\alpha) \ge d$ for all $\alpha \in F_q$. Since C is an optimal code, $R(C) \le d - 1$. Hence we have

$$d \le R(C_\alpha) \le R(C) + 1 \le d.$$

Thus $R(C) = d - 1$.■

3.2 Upper Bounds On $K_q(n,R)$.

Theorem 3.6. If some $(q,\ n,\ M)R$ seminormal code exists, then $K_q(n+q,\ R+q-1) \le M$.

Proof. Let A be a $(q,\ q,\ q)q - 1$ repetition code and let B be a $(q,\ n,\ M)R$ seminormal code with $\{B_\alpha\}_{\alpha\in F_q}$ an acceptable partition. For each $\alpha \in F_q$, let $A_\alpha = \{(\alpha,\alpha,\cdots,\alpha)\}$. Let $D = \bigcup_{\alpha\in F_q} D_\alpha$, where $D_\alpha = A_\alpha \oplus B_\alpha$. Then D, the **block wise direct sum of A and B,** is a $(q,\ n+q,\ M)$ code and by (2.9), $R(D) \ge R + q - 1$. To see that $R(D)$ is $R + q - 1$ we need to show that $d(x,D) \le R + q - 1$ for all $x \in F_q^{q+n}$. Let $x = (u,v)$; $u \in F_q^q$ and $v \in F_q^n$. If $d(v,B) \le R - 1$, there exists B_α with $d(v,B_\alpha) \le R - 1$ and hence $d(x,D) \le d(x,D_\alpha) = d(u,\ A_\alpha) + d(v,\ B_\alpha) \le q + R - 1$. If $d(v,B) = R$, then there exists B_α with $d(x,\ B_\alpha) = R$. Moreover, since B is seminormal, $d(v,B_\beta) \le R + 1$ for all $\beta \in F_q$. If $d(u,A) \le q-2$, then $d(u,\ A_\gamma) \le q - 2$ for some $\gamma \in F_q$. Therefore $d(x,D_\gamma) \le q - 2 + R + 1$ and hence $d(x,\ D)$

$\leq R + q - 1$. Finally if $d(u, A) = q - 1$, then $d(u, A_\alpha) = q - 1$ and hence $d(x, D) \leq d(x, D_\alpha) = R + q - 1$.■

Remark 3.3. In [32] Honkala has proved a similar theorem [Theorem 2, pp. 1204] with stronger assumption. Moreover our proof is simpler.

As an immediate corollary we have

Corollary 3.4. If some $(q, n, K_q(n, R))R$ seminormal code exists, then $K_q(n+q, R+q-1) \leq K_q(n, R)$.

Assumption of seminormality in the above theorem is necessary. For, if Theorem 3.6 is true for any code, then it follows from the fact "$K_3(3,1) = 5$ [39]" that $K_3(6,3) \leq 5$. But $K_3(6,3) = 6$ [47].

In Theorem 3.6, if in addition B is $(q, n, M)R$ strongly seminormal and A is a $(q,qt,q)t(q-1)$, $t \geq 1$, repetition code, then it is easy to verify that the block wise direct sum of A and B is a $(q, n+qt, M)R+t(q-1)$ code. Therefore $K_q(n+qt, R+t(q-1) \leq M$ for all $t \geq 1$.

Applying Proposition 2.19 to the codes given by Theorem 3.4 and Examples 3.1, 3.3, and 3.4, we get the following upper bounds.

Theorem 3.7. i) If q is prime power and $q \geq 4$, then

$$K_q(n+q, R+q-2) \leq qK_q(n, R).$$

ii) $K_3(n+10, R+5) \leq 9\, K_3(n, R)$.

iii) $K_5(n+5, R+3) \leq 5\, K_5(n, R)$.

Improvements on the previous known upper bounds given by

Theorem 3.7 and Tables I and III in [43] are summarized in the following corollary.

Corollary 3.5. $K_3(13,6) \le 45$ (48), $K_3(14,6) \le 81$ (102), $K_5(8,3) \le 325$ (455), $K_5(8,4) \le 65$ (121), $K_5(9,3) \le 1275$ (1625), $K_5(9,4) \le 255$ (325), $K_5(9,5) \le 55$ (65), $K_5(10, 3) \le 3600$ (6375), $K_5(10,4) \le 720$ (1225), $K_5(10,5) \le 175$ (255), $K_5(10,6) \le 45$ (55), $K_5(11,4) \le 3125$ (4375), $K_5(11,5) \le 625$ (875), $K_5(11,6) \le 125$ (175), $K_5(11,7) \le 25$ (45).

The numbers within parenthesis are earlier known bounds.

If C is a $(q,n,M)R$ code, then $D = C \oplus F_q$ is a $(q, n+1, qM)R$ strongly seminormal code with $\{D_\alpha\}_{\alpha \in F_q}$, where $D_\alpha = \{(c,\alpha) \mid c \in C\}$ an acceptable partition. Thus strongly seminormal codes of length greater than or equal to 9 can be constructed from the codes given by Corollary 3.5. But some of these may not be good covering codes. In order to get better upper bounds for $K_q(n, R)$, one needs to construct strongly seminormal codes of minimal cardinality.

Theorem 3.8. $K_q(q, q-2) \le 2q - 1$ for $q \ge 3$.

Proof. Let $q \ge 3$, $F_q = \{\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_q\}$ and let $\alpha \in F_q$, $\alpha \ne \alpha_q$. Let $x_1, x_2, \cdots, x_{2q-1} \in F_q^q$ be defined by

$$x_i = (\alpha_i, \alpha_i, \cdots, \alpha_i) \quad \text{for} \quad i = 1, 2, \cdots, q-1,$$

$$x_q = (\alpha, \alpha_q, \alpha_q, \cdots, \alpha_q), \quad x_{q+1} = (\alpha_q, \alpha, \alpha_q, \cdots, \alpha_q), \cdots,$$

$$x_{2q-1} = (\alpha_q, \cdots, \alpha_q, \alpha).$$

Then the covering radius of the code $C = \{x_1, x_2, \cdots, x_{2q-1}\}$ is atmost $q - 1$. If $R(C) = q - 1$, then there is a $y \in F_q^q$ such that

$d(y, C) = q - 1$. So y must have distinct coordinates. But then $d(y,x_i) = q - 2$ for some $i \in \{q, q+1, \cdots, 2q-1\}$, a contradiction. Thus $R(C) = q - 2$ and hence $K_q(q, q-2) \leq 2q - 1$ for $q \geq 3$.■

3·3 LOWER BOUNDS ON $K_q(n,R)$.

In recent years several authors viz. Honkala [31], van Wee [61], and others have determined lower bounds on $K_q(n,R)$ by dividing the set of all elements of F_q^n that lie in more than one sphere of radius R around the codewords to several classes and then by obtaining better estimates for the cardinality of some of these classes. The following observation gives a good lower bound on $K_q(n, R)$.

Theorem 3.9. If $0 \leq R_i \leq n_i$, $i = 1, 2$, then

$$K_q(n_1 + n_2, R_1 + R_2 + 1) \geq \min\{ K_q(n_1, R_1), K_q(n_2, R_2) \}.$$

Proof. Suppose C is a $(q, n_1 + n_2, M)R_1 + R_2 + 1$ code with $M < \min\{ K_q(n_1, R_1), K_q(n_2, R_2) \}$. Let $C = \{ (x_i,y_i) \mid 1 \leq i \leq M, x_i \in F_q^{n_1}$ and $y_i \in F_q^{n_2} \}$, $A = \{ x_i \mid (x_i,y_i) \in C \}$ and let $B = \{ y_i \mid (x_i,y_i) \in C \}$. Then the covering radius of A (B) is at least $R_1 + 1$ $(R_2 + 1)$. Since C is the concatenation of codes A and B, by (2.9), $R(C) \geq R_1 + R_2 + 2$, a contradiction.■

The following corollary follows immediately by induction

Corollary 3.6. If $0 \leq R_i \leq n_i$, $i = 1, 2, \cdots , t$, then

$$K_q\left(\sum_{i=1}^{t} n_i , \sum_{i=1}^{t} R_i + (t-1)\right) \geq \min_i\{ K_q(n_i, R_i) \}.$$

The following corollary shows that the lower bounds given by Corollary 3.6 are at times better.

Corollary 3.7. $K_3(9,5) \geq 5$ (4), $K_3(11,6) \geq 6$ (5)

$K_3(13,7) \geq 6$ (5), $K_3(12,7) \geq 6$ (4), $K_3(14,8) \geq 6$ (4),

$K_4(8,5) \geq 7$ (5), $K_4(9,5) \geq 8$ (7), $K_4(10,6) \geq 7$ (5),

$K_5(6,3) \geq 13$ (11), $K_5(7,4) \geq 9$ (8), $K_5(8,5) \geq 9$ (6),

$K_5(9,6) \geq 8$ (6).

By Corollary 3.6, $K_q(qr, qr-r-1) \geq K_q(q, q-2)$. On the other hand by Proposition 2.20, $K_q(qr, qr-r-1) \leq 2q$. Therefore

$$(3.4) \qquad K_q(q, q-2) \leq K_q(qr, qr-r-1) \leq 2q$$

If $q = 2$, then the inequality (3.4) gives $K_2(2r, r - 1) = 4$, a result of Cohen et al [12]. If $q=3$ and $r = 2n$, then by inequality (3.4), $K_3(6n, 4n - 1) \leq 6$. Since $K_3(6, 3) = 6$ [39], by Corollary 3.6, $K_3(6n, 3n+n-1) \geq K_3(6, 3) = 6$. Thus we have

Theorem 3.10. For any positive integer n, $K_3(6n,4n-1) = 6$.

Since $K_4(4, 2) = 7$ [47], by inequality (3.4),

$$7 \leq K_4(4n, 3n - 1) \leq 8 \text{ for all } n \geq 1.$$

Techniques used in Theorem 3.9 are easily extendable to mixed codes.

Theorem 3.11. If $m = m_1 + m_2$, $n = n_1 + n_2$ and $R = R_1 + R_2 + 1$, then $K_{q_1,q_2}(n, m; R) \geq \min\{ K_{q_1,q_2}(n_1, m_1; R_1), K_{q_1,q_2}(n_2, m_2; R_2) \} = M$.

Proof. Suppose not. Then there is a code $C = \{ (x_i, y_i) \mid x_i \in F_{q_1}^{n_1} F_{q_2}^{m_1}, y_i \in F_{q_1}^{n_2} F_{q_2}^{m_2}$ and $1 \leq i \leq N < M \}$. Let $A = \{ x_i \mid (x_i, y_i) \in$

C } and let $B = \{ y_i \mid (x_i, y_i) \in C \}$. Then the covering radius of A (B) is at least $R_1 + 1$ ($R_2 + 1$) and C is the concatenation of codes A and B. Since C is a concatenation of the codes A and B, by (2.9), $R(C) \geq R_1 + R_2 + 2$, a contradiction.■

As an immediate Corollary we have

Corollary 3.8. (i) $K_{q_1,q_2}(2n , 2m; 2R + 1) \geq K_{q_1,q_2}(n , m; R)$,

ii) $K_{q_1,q_2}(n, m; R) \geq \min\{ K_{q_1}(n, R_1), K_{q_2}(m, R_2) \}$, where $R = R_1 + R_2 + 1$.

If $q_1 = 3$ and $q_2 = 2$, then Theorem 3.11 and the Table in [27], give the following bounds.

Corollary 3.9. $K_{3,2}(4 , 2; 3) = 4$, $K_{3,2}(2 , 4; 3) = 3$,

$K_{3,2}(3, 2; 3) = 3$, $K_{3,2}(2 , 2; 2) = 3$, $K_{3,2}(4 , 1; 3) = 3$,

$K_{3,2}(3, 2; 3) \geq 3$, $K_{3,2}(2n , n; 2n - 1) \geq K_{3,2}(2 , 1; 1) \geq 4$,

$$K_{3,2}(n ,2n; 2n - 1) \geq K_{3,2}(1 , 2; 1) \geq 3.$$

The code constructed in this Chapter can be used to determine the value of $l(m,R; q) = \min \{ n \mid$ there is an $[n,n-m]R$ q-ary linear code $\}$ for some m and R.

Theorem 3.12. If $q \geq 3$ and a prime power, then $l(q - 1, q - 2; q) = q + 1$.

Proof. By Theorem 3.2, Theorem 3.3 and Example 3.1, there is a $[q+1, 2]q-2$ q-ary code for $q \geq 4$. If $q=3$, then $S_2(3)$ is a $[4, 2]1$ ternary code [19]. Therefore $l(q-1, q-2; q) \leq q + 1$ for $q \geq 3$. Suppose $l(q-1,q-2;q) \leq q$. Then there exists a $[q, 1]$ linear code C with covering radius $q-2$. Since the covering radius of any code with q codewords of length n lies between $\lfloor n(q-1)/q \rfloor$ and n, $q-1 \le R(C) \le q$, a contradiction.∎

We need the following Lemma to show that $l(3, 2; 5) = 6$. Recall that $t_q[n, k] = \min \{ R \mid$ there is an $[n, k]R$ q-ary linear code $\}$.

<u>**Lemma 3.10.**</u> $t_5[5, 2] = 3$.

<u>**Proof.**</u> Let C be a $[5, 2, d]$, $1 \le d \le 4$, code over GF(5), then by redundancy bound, $R(C) \le 3$. If $d = 4$, then C is equivalent to punctured Simplex code. Therefore by Theorem 3.1, $R(C) = 3$. If $d = 3$, then C is a $[5, 2, 3]$ code. By using MacWilliams identities (2.3), we get the following two sets of weight distribution for C

A_0	A_3	A_4	A_5
1	4	12	8
1	8	4	12

These codes are equivalent to the codes C_1 and C_2 generated by the matrices

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & \alpha_3 & \alpha_3 & \alpha_4 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & \alpha_3 & \alpha_3 & \alpha_5 \end{bmatrix},$$

respectively. A simple verification shows $R(C_1) = 3 = R(C_2)$.

If $d = 2$, then the MacWilliams identities (2.3) give the following set of weight distributions:

A_0	A_2	A_3	A_4	A_5
1	4	0	8	12
1	4	4	0	16

These weight distributions give codes C_3 and C_4 with generator matrices

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & \alpha_3 & \alpha_3 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & \alpha_3 & \alpha_4 \end{bmatrix},$$

respectively. It is easy to verify that $R(C_3) = 3 = R(C_4)$.

If $d = 1$, then by MacWilliams identity (2.3), the weight distribution is $A_0 = 1$, $A_1 = 4 = A_4$, $A_5 = 16$. So the code C is equivalent to the code generated by the matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Let $x = (0, 1, \alpha_3, \alpha_4, \alpha_4) \in F_5^5$, then the $d(x, C) = 3$ and hence $R(C) \geq 3$. Therefore by redundancy bound (2.6), $R(C) = 3$. Hence any $[5, 2, d]$, $1 \leq d \leq 4$, code over F_5 has covering radius 3, that is, minimum possible covering radius of a [5, 2] code over F_5 is 3.■

Theorem 3.13. $l(3, 2; 5) = 6$.

Proof. By Example 3.3, $l(3, 2; 5) \leq 6$. Suppose $l(3, 2; 5) \leq 5$. Then there is a $[5, 2]2$ code over F_5 and hence $t_5[5, 2] \leq 2$, a contradiction to Lemma 3.9. Therefore $l(3, 2; 5) = 6$.■

Chapter IV

Optimal Codes of Dimension 3, 4 and 5

In this Chapter we determine $n_q(k,d)$, the minimum length of a q-ary linear code of dimension k and minimum distance d, for smaller k and some d. Throughout this Chapter q is a prime power and an [n,k,d] code will mean a q-ary linear code.

4.1 BOUNDS ON $n_q(3,2q)$.

If C is an $[n_q(k,d+1),k,d+1]$, $d \geq 1$, code, then by puncturing a suitable coordinate of it, one gets an $[n_q(k,d+1)-1, k, d]$ code and hence

(4.1) $$n_q(k,d) \leq n_q(k,d+1) - 1$$

Thus $n_q(k, d)$ is a strictly increasing function of d. In [14], Dodunekov has determined the value of $n_q(3, d)$ for $d \leq q + 2$ (Proposition 2.8) and has also shown that $n_q(3,q(q-2)) = g_q(3,q(q-2))+1$. If $3 \nmid q$, then the following theorem gives a lower bound for $n_q(3,2q)$

Theorem 4.1. If $3 \nmid q$, then $n_q(3, 2q) \geq g_q(3, 2q) + 1$.

Proof. Suppose $n_q(3, 2q) = g_q(3,2q) = 2q + 3$. Then there exists a $[2q+3,3,2q]$ code C. Since $2q \leq q^2$ and C meets the Griesmer bound, by Proposition 2.5, $B_1 = 0 = B_2$. The MacWilliams identities (2.3) give

$$\begin{aligned} A_{2q} + A_{2q+1} + A_{2q+2} + A_{2q+3} &= q^3-1 \\ 3A_{2q} + 2A_{2q+1} + A_{2q+2} &= (q^2-1)(2q+3) \\ 3A_{2q} + A_{2q+1} &= (q^2-1)(2q+3) \end{aligned}$$

Solving these equations one gets, $A_{2q} = \frac{(q^2-1)(2q+3)}{3}$, $A_{2q+1} = 0$, $A_{2q+2} = 0$ and $A_{2q+3} = \frac{q(q-1)(q-2)}{3}$. So C has a generator matrix of the form

$$G = \begin{bmatrix} 0 & x \\ 0 & y \\ 1 & z \end{bmatrix}$$

where $w(x) = w(y) = 2q$ and $w(z) = 2q + 2$. Last two rows of G generate a $[2q+3,\ 2,\ 2q]$ code A. Let $\{A'_i\}_{i=0}^{n}$ and $\{B'_i\}_{i=0}^{n}$ be the weight distributions of the code A and $A^{\perp}$, respectively. Since the generator matrix of A has no zero column, $B'_1 = 0$. Moreover, since A is a subcode of C, $A'_{2q+1} = A'_{2q+2} = 0$. Therefore MacWilliams identities (2.2) give

$$\begin{aligned} A'_{2q} + A'_{2q+3} &= q^2 - 1 \\ 3A'_{2q} &= (2q+3)(q-1) \end{aligned}$$

Solving above equations, one gets $A'_{2q} = (q-1)\frac{2q+3}{3}$ and $A'_{2q+3} = (q-1)\frac{q}{3}$. Since each A'_i is a multiple of q-1, $q \equiv 0 \pmod 3$, a contradiction to the hypothesis. Hence the Theorem.∎

Let A be a $[q+4,3,q+1]$ code and let B be a $[q+1,3,q-1]$ code.

Then the concatenation of A and B give a [2q+5, 3, 2q] code C and hence $n_q(3,2q) \le 2q + 5$. Therefore by Theorem 4.1,

$$(4.2) \qquad 2q + 4 \le n_q(3,2q) \le 2q + 5 \text{ for } q \not\equiv 0 \pmod 3)$$

The following corollary gives the value of $n_q(3,2q)$ for q even.

<u>**Corollary 4.1**</u>. If q is even, then $n_q(3,2q) = g_q(3,2q) + 1$.

<u>**Proof.**</u> Let D be a [q+2,3,q] code [14]. Then the code $C = \{(x,x) \mid x \in D\}$ is a [2q+4, 3, 2q] linear code and hence by inequality (4.2), $n_q(3,2q) = g_q(3,2q) + 1$.■

If q = 3, then $n_3(3, 6)$ reaches the Griesmer bound, but for q = 5 and 7, $n_q(3, 2q) = g_q(3, 2q) + 1$ [29]. The following three Examples show that Corollary 4.1 is also true for q = 11, 13 and 17.

Example 4.1. The matrix

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 0 & 1 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 0 & 0 \\ 0 & 0 & 1 & 3 & 2 & 5 & 4 & 1 & 7 & 6 & 10 & 8 & 5 & 3 & 6 & 7 & 3 & 0 & 0 & 5 & 2 & 2 & 4 & 9 & 1 & 1 \end{bmatrix}$$

with entries from $\mathbb{Z}_{11}$ generates a [26,3,22] code over $\mathbb{Z}_{11}$. Hence by (4.2), $n_{11}(3, 22) = 26$.

Example 4.2. The code generated by the matrix

$$\begin{bmatrix} 1&0&1&1&1&1&1&1&1&1&1&1&1&1&1&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 0&1&1&2&3&4&5&6&7&8&9&10&11&12&0&1&0&1&1&2&3&4&5&6&7&8&9&10&11&12 \\ 0&0&1&3&2&5&4&2&6&0&5&3&12&4&10&8&11&11&10&7&8&1&5&4&1&8&3&7&2&8 \end{bmatrix}$$

over $\mathbb{Z}_{13}$ is a [30,3,26] 13-ary code. Hence by (4.2), $n_{13}(3,26)=30$.

Example 4.3. The code generated by the matrix

$$\begin{bmatrix} 1&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0&0 \\ 0&1&1&2&3&4&5&6&7&8&9&10&11&12&13&14&15&16&0&1&1&2&3&4&5&6&7&8&9&10&11&12&13&14&15&16&0&0 \\ 0&0&1&3&2&5&4&8&11&6&9&1&16&7&14&12&9&6&11&8&10&4&5&15&2&0&6&4&16&2&9&5&10&0&11&7&1&1 \end{bmatrix}$$

over $\mathbb{Z}_{17}$ is a [38, 3, 34] code. Hence by (4.2), give $n_{17}(3, 34) = 38$.

It is conjectured that the Corollary 4.1 is true for all $q \not\equiv 0 \pmod 3$.

Example 4.4. 9-ary code generated by the matrix

$$\begin{bmatrix} 1&1&0&1&1&1&1&1&1&0&\alpha_5&\alpha_9&\alpha_9&1&\alpha_3&\alpha_9&0&\alpha_8&\alpha_4&\alpha_3&\alpha_8&\alpha_4 \\ 1&\alpha_4&\alpha_3&1&\alpha_5&\alpha_6&\alpha_7&\alpha_8&\alpha_9&0&0&0&1&1&1&1&1&1&1&1&0&\alpha_5 \\ 0&\alpha_7&\alpha_7&1&\alpha_3&\alpha_4&1&\alpha_4&\alpha_3&1&1&0&\alpha_7&\alpha_7&1&\alpha_3&\alpha_4&1&\alpha_4&\alpha_3&\alpha_7&1 \end{bmatrix}$$

is a [22,3,18] code. Therefore by inequality (2.4), $n_9(3,18) = 21$ or 22.

4.2 Bounds on $n_q(4,d)$.

In [21], Greenough and Hill have determined $n_4(4,d)$ for all but 10 values of d. These 10 cases have since been resolved. In this section we determine $n_q(4,d)$ for a general q and some d.

Theorem 4.2. $n_q(4,q^2-i) \le g_q(4,q^2-i)+1$, for $1 \le i \le q-1$.

Proof. Let A be a $[q^2+1,4,q^2-q]$ two-weight code having a codeword of weight q^2 [8]. Then A has a generator matrix of the form

$$G_A = \left[\begin{array}{c|c} 0 & 1 \quad 1\ldots.1 \\ 1 & x \\ 0 & x' \\ 0 & x'' \end{array}\right]. \tag{4.3}$$

For each i, $1 \le i \le q-1$, let D_i be a $[q+2-i,\ 3,\ q-i]$ code with generator matrix G_i [14]. Then the matrix

$$G = \left[\begin{array}{c|c} 0\ 0\ \cdots\ 0 & \\ & G_A \\ G_i & \end{array}\right] \tag{4.4}$$

generates a $[q^2+q+3-i,\ 4,\ q^2-i]$ code C.■

As an immediate corollary we have

Corollary 4.2. If q is even, then $n_q(4,q^2) \le g_q(4,q^2)+1$.

Proof. Let q be even and let D be a $[q+2,3,q]$ code with generator matrix G_D [14]. Let G be the matrix given by (4.4) on replacing G_i by G_D . Then G generates a $[q^2+q+3,\ 4,\ q^2]$ code.■

The following Theorem gives exact value of $n_q(4,q^2-2)$.

Theorem 4.3. If $q \ge 3$, then $n_q(4,q^2-2) = q^2+q+1$.

Proof. If possible, let C be an $[n,4,d]$ code where $n = q^2+q$ and $d = q^2-2$. Then $A_w = 0$ for $w = d+i$, $3 \le i \le q$. For, if $A_w \ne 0$ for some i, then by Proposition 2.9, Res(C, w) is a $[q+2-i,\ 3,\ q+1-i]$ code. But by (2.4), such a code does not exist. Hence possible nonzero weights in C are d, d+1, d+2, n-1 and n. By Proposition 2.5, $B_j = 0$ for j = 1, 2, 3. The MacWilliams identities (2.3) give

$$A_d + A_{d+1} + A_{d+2} + A_{n-1} + A_n = q^4 - 1$$

$$(q+2)A_d + (q+1)A_{d+1} + qA_{d+2} + A_{n-1} = (q^3-1)n$$

$$(q+2)(q+1)A_d + (q+1)qA_{d+1} + q(q-1)A_{d+2} = (q^2-1)n(n-1)$$

$$(q+2)(q+1)qA_d + (q+1)q(q-1)A_{d+1} + q(q-1)(q-2)A_{d+2} = (q-1)n(n-1)(n-2).$$

By (2.5), one of A_n and A_{n-1} must be zero. Moreover if $A_n \neq 0$, then $A_n = q - 1$. Thus if $A_n = q-1$ and $A_{n-1} = 0$, solving the above equations one gets $A_{d+1} < 0$ for $q \geq 3$, a contradiction. Hence $A_n = 0$. If $A_{n-1} \neq 0$, then solving above system of equations again we get $A_{d+2} < 0$ for $q \geq 3$, a contradiction. Therefore $n_q(4,\ q^2-2) \geq g_q(4,\ q^2-2) + 1$ and hence by Theorem 4.2, proof is complete.∎

By Proposition 2.7 and Theorem 4.3, we have

(4.5) $$n_q(4,q^2-i) \geq g_q(4,q^2-i)+1 \text{ for } 0 \leq i \leq 2 \text{ and } q \geq 3.$$

Hence by Theorem 4.2 and inequality (4.5), the following theorem follows.

Theorem 4.4. If $q \geq 3$, then $n_q(4,\ q^2-i) = g_q(4,\ q^2-i)+1$ for i = 1 and 2.

For odd q, similar technique gives the value of $n_q(4,\ q^2-i)$ for $1 \leq i \leq q-1$.

Theorem 4.5. If q is odd, then $n_q(4,q^2-i) = g_q(4,q^2-i) + 1$ for $1 \leq i \leq q-1$.

Proof. By Theorem 4.2, $n_q(4, q^2- i) \le g_q(4, q^2- i) + 1$ for $1 \le i \le q - 1$. If $n_q(4, q^2- q + 1) = g_q(4, q^2- q + 1) = q^2 + 3$, let C be a $[q^2+3, 4, q^2-q+1]$ code. By Proposition 2.9, the residual code of C with respect to a codeword of weight $q^2 - q + 1$ is a $[q+2, 3, q]$ code. But by Proposition 2.8, such a code does not exist for odd q. Therefore $n_q(4,q^2- q + 1) = g_q(4,q^2- q + 1) + 1$. Hence by Proposition 2.7, the theorem follows.∎

By Corollary 4.2 and inequality (4.5), we have

Corollary 4.3. If q is even, then $n_q(4,q^2) = g_q(4,q^2) + 1$.

Theorem 4.6. If q is odd, then $q^2+q+3 \le n_q(4,q^2) \le q^2+q + 4$.

Proof. Let A be a $[q^2+1, 4, q(q-1)]$ q-ary code generated by the matrix G_A given by (4.3). If B is a $[q+3, 3, q]$ code with a generator matrix G_B [14], then the matrix

$$G = \left[\begin{array}{c|c} G_A & \begin{array}{ccccc} 0 & 0 & \cdots & & 0 \\ & & G_B & & \end{array} \end{array}\right]$$

generates a $[q^2+q+4, 4, q^2]$ code. Hence $n_q(4,q^2) \le q^2+ q + 4$. If $n_q(4,q^2) = q^2+ q + 2$, let C be a $[q^2+ q + 2, 4, q^2]$ code. Then a punctured code of C is a $[q^2+ q + 1, 4, q^2- 1]$ code. Therefore $n_q(4, q^2-1) = q^2 + q + 1$, a contradiction to Theorem 4.5. Hence $n_q(4, q^2) \ge q^2 + q + 3$.∎

Theorem 4.7. For $2 \le i \le q - 2$, $n_q(4,q(q-i)) \ge g_q(4,q(q-i)) + 1$.

Proof. Suppose $n_q(4, q(q-i)) = g_q(4, q(q-i))$ for some i. Let $d = q(q-i)$, $n = g_q(4,d) = (q+1)(q-i)+2$ and let C be an $[n, 4, d]$ code. Then $A_w = 0$ for $w = d+1, d+2,\cdots, d+q-i$. For, if $A_w \ne 0$ for some $w = d + j$, $1 \le j \le q - i$, then by Proposition 2.9, Res(C,w) is an

$[n-w, 3, q-i-j+1]$ code. But by (2.4), such a code does not exist. Therefore possible non-zero weights in C are $\{d, n-1, n\}$. Since the code meets the Griesmer bound, by Proposition 2.5, $B_1 = B_2 = 0$. The MacWilliams identities (2.3) for B_0, B_1 and B_2 give

$$A_d + A_{n-1} + A_n = q^4 - 1$$

$$(q-i+2)A_d + A_{n-1} = n(q^3 - 1)$$

$$\binom{q-i+2}{2}A_d = \binom{n}{2}(q^2 - 1)$$

Solving these equations one gets $A_d = \dfrac{n(n-1)(q^2-1)}{(q-i+2)(q-i+1)}$, $A_{n-1} = \dfrac{n(q-1)iq}{(q+1-i)}$ and $A_n = \dfrac{-q(q-1)(i-1)(q^2-(i+1)q-i)}{q-i+2}$. Thus $A_n < 0$ for $q \geq 4$, a contradiction. Hence the theorem follows.■

Since $n_q(4, q(q-1)) = q^2 + 1$ [8], by inequality (4.1), $n_q(4,q(q-2)) \leq n_q(4,q(q-2)+q) - q = q^2 + 1 - q = g_q(4,q(q-2)) + 1$ and hence by Theorem 4.7, we get

Theorem 4.8. $n_q(4,q(q-2)) = g_q(4,q(q-2)) + 1$ for $q \geq 4$.

4.3 Bounds on $n_4(5,d)$.

In [5] Bhandari and Garg and in [21] Greenough and Hill have independently determined the value of $n_4(4,d)$. In this section we determine lower bounds on $n_4(5,d)$ and construct some codes to get exact value of $n_4(5, d)$ for some small d's. We first prove some results on $n_q(k, d)$ that are useful in showing nonexistence of certain codes.

Lemma 4.4. Let C be an [n, k, d] code with generator matrix G and let $d \le q^{k-1}$. If $n = g_q(k,d) + t$, $t \ge 0$, then any column of G is repeated atmost t+1 times.

Proof. If G has a column that appears more than t+1 times, then it is equivalent to the matrix

$$G' = \left[\begin{array}{c|c} \overset{\longleftarrow\; t+2 \;\longrightarrow}{1\ \ 1\ \ .\ \ .\ \ .\ \ 1} & x \\ & \\ 0 & A \end{array}\right]$$

Then the matrix A generates an $[n-t-2, k-1, d']$, $d' \ge d$, code. But by (2.4), such a code does not exist. Hence every column of G is repeated atmost t+1 times.∎

Lemma 4.5. Let C be an [n, k, d] code and let G be a generator matrix for C. If G has no zero column and has exactly one column that appears more than once, say s times, then $B_2 = (q-1)s(s-1)/2$.

Proof. G is equivalent to the matrix

$$G' = \left[\begin{array}{c|c|c} \overset{\longleftarrow\; s \;\longrightarrow}{1\ \ 1\ \ \cdot\ \ \cdot\ \ \cdot\ \ 1} & 0\ \cdots\ 0 & \\ & I_{k-1} & B \\ 0 & & \end{array}\right]$$

Hence a generator matrix for $C^{\perp}$ is equivalent to the matrix

$$H' = \left[\begin{array}{c|c} & \begin{array}{cc} 1 & \\ \vdots & 0 \\ 1 & \end{array} \\ I_{n-k} & \\ \hline & B^t \end{array}\right] \begin{array}{l} \Big\updownarrow s-1 \\ \\ \\ \end{array} = \left[\begin{array}{c} u_1 \\ u_2 \\ \vdots \\ u_{n-k} \end{array}\right]$$

where B^t is the transpose of the matrix B. Since any two columns of B are linearly independent, any linear combination of the rows of H′ that contains one or more of u_j's, $s \le j \le n-k$, has weight 3 or more. Thus the elements of $C^{\perp}$ of weight 2 are of the type αu_i or $\alpha(u_i - u_j)$ where $\alpha \in F_q \backslash \{0\}$, $1 \le i < j \le s - 1$. Hence $B_2 = (s-1)(q-1) + \binom{s-1}{2}(q-1)$.■

Theorem 4.9. Let $d \le q^{k-2}$ and let $n = g_q(k, d) + 1$. If C is an [n, k, d] code with generator matrix G, Then G has atmost one column that appears twice and $B_2 = 0$ or $q - 1$.

Proof. By Lemma 4.3, no column of G appears more than twice. If some two columns, say, ith and jth, appears twice, then G is equivalent to the matrix

$$G' = \left[\begin{array}{cccc|c} 1 & 1 & 0 & 0 & x \\ 0 & 0 & 1 & 1 & y \\ \hline & & 0 & & A \end{array}\right]$$

where $x, y \in F_q^{n-4}$. The matrix A generates a $[g_q(k, d)-3, k-2, d_1]$ $d_1 \ge d$, q-ary code. But by (2.4), such a code does not exist. Therefore atmost one column repeats twice and hence by Lemmas 4.4, $B_2 = 0$ or $q - 1$.■

The following Lemma gives a lower bound to $n_q(k,d)$ in general

Lemma 4.6. If $n_q(k, d) \ge g_q(k, d) + t$, then $n_q(k+1, qd-i) \ge g_q(k+1, qd-i) + t$, $0 \le i \le q-1$.

Proof. If $n_q(k+1, qd-i) \le g_q(k+1, qd-i) + t - 1$ for some i, let C be a $[g_q(k+1,qd-i)+t-1, k+1, qd-i]$ q-ary code. Then Res(C, qd-i) is a $[g_q(k+1,qd-i)+t-1-(qd-i), k, d]$ code. Therefore

$$\begin{aligned} g_q(k,d) + t &\le n_q(k,d) \\ &\le g_q(k+1, qd-i) + t - 1 - (qd-i) \\ &= \sum_{j=0}^{k} \lceil (qd-i)/q^j \rceil + t - 1 - (qd-i) \\ &= \sum_{j=1}^{k} \lceil (qd-i)/q^j \rceil + t - 1 = \sum_{j=1}^{k} \lceil (d-i/q)/q^{j-1} \rceil + t - 1 \\ &= \sum_{j=0}^{k-1} \lceil (d-i/q)/q^j \rceil + t - 1 = \sum_{j=0}^{k-1} \lceil (d/q^j) - (i/q^{j+1}) \rceil + t - 1 \\ &\le \sum_{j=0}^{k-1} \lceil d/q^j \rceil + t - 1 = g_q(k,d) + t - 1, \end{aligned}$$

a contradiction. Hence $n_q(k+1, qd-i) \ge g_q(k+1, qd-i) + t$, $0 \le i \le q-1$. ■

Using above lemma and the lower bounds from the Table in [21], we get the following.

Theorem 4.10. If $d \in \{ i \mid 9 \le i \le 16,\ 25 \le i \le 32,\ 49 \le i \le 64,\ 89 \le i \le 128,\ 145 \le i \le 176 \}$, then $n_4(5,d) \ge g_4(5,d) + 1$.

Let G be the 5 × 10 matrix over F_4 given by

$$G = \left[\begin{array}{cccc|cccccc} 1 & 1 & 1 & 1 & \alpha_3 & \alpha_3 & \alpha_4 & 1 & 0 & 0 \\ & & & & 0 & 1 & 1 & 1 & 1 & 0 \\ & & I_4 & & 0 & 0 & \alpha_4 & \alpha_4 & \alpha_3 & 1 \\ & & & & 0 & 1 & 0 & \alpha_3 & 1 & \alpha_3 \\ & & & & 0 & 1 & \alpha_4 & 0 & \alpha_4 & \alpha_3 \end{array}\right].$$

Then G generates a [10,5,5] code C. It meets the Griesmer bound. On successively puncturing C, we get [9, 5, 4] and [8, 5, 3] quaternary codes. Hence by inequality (4.1) and table in [12], $n_4(5, d) \ge g_4(5,d) + 1$ for d = 3 and 4. Hence we have the following theorem follows.

Theorem 4.11. $n_4(5,5) = 10$, $n_4(5,4) = 9$ and $n_4(5,3) = 8$.

The following two theorems show that [29,5,20] and [49,5,3 quaternary codes do not exist.

Theorem 4.12. $n_4(5,20) \geq g_4(5,20) + 1$.

Proof. Suppose $n_4(5, 20) = g_4(5, 20) = 29$. Let C be a [29, 5, 2 quaternary code. By constructing suitable residual codes, it easy to verify that $A_i = 0$ for $i \in \{ 21, 22, 23, 25 \}$ and Proposition 2.10, $A_{26} = 0$. Therefore possible nonzero weights a $\{ 20, 24, 27, 28, 29 \}$. By (2.4), $A_{29} = 0$ or $A_{28} = 0$ Thus if A $\neq 0$, then $A_{29} = 3$ and $A_{28} = 0$. By Proposition 2.5, $B_j = 0$ for j 1, 2, 3. First three MacWilliams identities (2.3) give

$$\begin{aligned} A_{20} + A_{24} + A_{27} &= 4(4^4 - 1) \\ 9A_{20} + 5A_{24} + 2A_{27} &= 29(4^4 - 1) \\ 36A_{20} + 10A_{24} + A_{27} &= 406(4^3 - 1) \end{aligned}$$

Solving these system of equations, one gets $A_{20} = 8493/14$, contradiction. Therefore $A_{29} = 0$. Then the MacWilliams identiti (2.3) give

$$\begin{aligned} A_{20} + A_{24} + A_{27} + A_{28} &= 4^5 - 1 \\ 9A_{20} + 5A_{24} + 2A_{27} + A_{28} &= 29(4^4 - 1) \\ 36A_{20} + 10A_{24} + A_{27} &= 406(4^3 - 1) \\ 84A_{20} + 10A_{24} &= 3654(4^2 - 1) \end{aligned}$$

Again solving these equations, one gets $A_{20} = 4275/7$, contradiction. Therefore our supposition is wrong and hence t

Theorem.■

Theorem 4.13. $n_4(5,35) \geq g_4(5,35) + 1 = 50$.

Proof. Suppose $n_4(5, 35) = 49$. Let C be a $[49, 5, 39]$ code over F_4 . By considering residual codes of suitable codewords, it is easy to verify that $A_i = 0$ for $i \in \{ 37, 38, 41\text{-}43, 45 \}$ and by Proposition 2.10, $A_{46} = 0$. Therefore only possible nonzero weights are $\{ 35, 36, 39, 40, 44, 47\text{-}49 \}$. Since the code C meets the Griesmer bound, by Proposition 2.5, $B_j = 0$ for $j = 1, 2, 3$. The first four MacWilliams identities (2.3) give

$$\begin{aligned}
A_{35} + A_{36} + A_{39} + A_{40} + A_{44} + A_{47} + A_{48} + A_{49} &= 1023\\
14A_{35} + 13A_{36} + 10A_{39} + 9A_{40} + 5A_{44} + 2A_{47} + A_{48} &= 12495\\
91A_{35} + 78A_{36} + 45A_{39} + 36A_{40} + 10A_{44} + A_{47} &= 74088\\
364A_{35} + 286A_{36} + 120A_{39} + 84A_{40} + 10A_{44} &= 276360
\end{aligned}$$

By Proposition 2.4, $A_i = 0$ or 3 for $i \geq 47$. If $A_{49} = 3$, then by equation (2.5), $A_j = 0$ for $j \geq 43$. By solving the above system of equations, we get

$$18A_{35} + 12A_{36} - 2A_{40} = 12123$$

The left hand side of this equation is congruent to 0 modulo 2 but right hand side is congruent to 1 modulo 2, a contradiction. Hence $A_{49} = 0$. If $A_{48} = 3$, then by Proposition 2.4, $A_j = 0$ for $j \geq 44$. By solving the above system of equations we get $10A_{35} + 6A_{36} = -65870$, a contradiction to A_i is a nonnegative integer. Therefore $A_{48} = 0$. Similarly $A_{47} = 0$. So the possible nonzero weight vectors are $\{35, 36, 39, 40, 44\}$. Solving the above system

$3(1097-t)/7$, $A_{47} = 18(12963-2t)$ and $A_{46} < 0$, a contradiction. Therefore $A_{61} = 0$. Similarly if $A_{60} = 3$, then by Proposition 2.4, $A_j = 0$ for $j \geq 54$ and solving the above system of equations again we get $6A_{48} + 210A_{52} = -69433$, a contradiction. Therefore $A_{60} = 0$. Thus possible nonzero weights are $\{ 45\text{-}48, 52 \}$. The above system of equations now give $6A_{48} + 210A_{52} = -61380$, a contradiction to A_i integer. Therefore the above system of equation don't have a positive integer solution and hence $n_4(5,45) \geq g_4(5,45) + 1$.■

Using Theorem 4.14 and Proposition 2.7, we get

(4.6) $\qquad n_4(5,45+i) \geq g_4(5,45+i) + 1$ for $0 \leq i \leq 3$.

and by inequality (4.1) and Table in [21], we get

$n_4(5,d) \geq g_q(5,d) + 1$ for $d \in \{ 3, 4, 7, 8 \} \cup \{ i \mid 13 \leq i \leq 16, 23 \leq i \leq 32, 37 \leq i \leq 44, 77 \leq i \leq 80 \}$.

For $d = 64$, the following theorem gives a further improvement

Theorem 4.15. $n_4(5,64) \geq 88$.

Proof. Suppose not. Then there exists a [87,5,64] code over F_4 . By Proposition 2.9, possible nonzero weights are $i \in \{ 64, 70\text{-}72, 86, 87 \}$. The MacWilliams identity (2.3) for B_0, B_1 and B_2 give,

$$\begin{aligned}
A_{64} + A_{70} + A_{71} + A_{72} + A_{86} + A_{87} &= 1023 \\
23A_{64} + 17A_{70} + 16A_{71} + 15A_{72} + A_{86} &= 22185 \\
253A_{64} + 136A_{70} + 120A_{71} + 105A_{72} &= 235686 + 64B_2
\end{aligned}$$

By Proposition 2.4, $A_i = 0$ or 3 for $i > 78$. If $A_{87} \neq 0$, then $A_{87} = 3$ and $A_j = 0$ for $j \in \{ 70\text{-}72, 86 \}$. Hence by solving the above system of equations, we get $A_{64} = 22185/23$, a contradiction.

Therefore $A_{87} = 0$. If $A_{86} \neq 0$, then $A_{86} = 3$ and $A_j = 0$ for $j \in \{71, 72, 87\}$. Then the above equations give $A_{64} = 807$ and $A_{70} = 213$. This implies $B_2 < 0$, a contradiction. So $A_{86} = 0$. Therefore the only possible non-zero weights are $\{64, 70\text{-}72\}$. By solving the above equations again we get

$$\begin{aligned} 8A_{64} + 2A_{70} + A_{71} &= 6840 \\ 28A_{64} + A_{70} &= 25668 + 64B_2 \end{aligned}$$

This implies

$$25668 + 64B_2 \leq 28(8A_{64} + 2A_{70} + A_{71}) = 20520$$

a contradiction. Hence $n_4(5,64) \geq g_4(5,64) + 2$.■

Chapter V

Covering Radius of Simplex and Macdonald Class

In this chapter, we determine the covering radius of two optimal codes, namely, Simplex and MacDonald codes. These codes were defined in Chapter II. Throughout this Chapter $F_q = \{\alpha_1 = 0, \alpha_2 = 1, \alpha_3, \cdots, \alpha_q \}$ is a finite field.

5.A The Covering Radius of Simplex Code.

Let $S_k(q)$ be a k-dimensional Simplex code over F_q. It was seen in Chapter II that a generator matrix $G_{k+1}(q)$ for $S_{k+1}(q)$ can be defined inductively by (2.2), that is

$$(5.1) \quad G_{k+1}(q) = \left[\begin{array}{c|c|c|c|c|c} 00\cdots0 & 1 & 11\cdots1 & \alpha_3\cdots\alpha_3 & \cdots & \alpha_q\cdots\alpha_q \\ \hline & 0 & & & & \\ G_k(q) & 0 & G_k(q) & G_k(q) & \cdots & G_k(q) \\ & \vdots & & & & \\ & 0 & & & & \end{array}\right]$$

$S_k(q)$ is a $[(q^k-1)/(q-1),\ k,\ q^{k-1}]$ code that meets the Griesmer bound. If $q = 2$, the covering radius of the binary Simplex code $S_k(2)$ is $2^{k-1} - 1$. If $q > 2$, then very little is known about the covering radius of $S_k(q)$. In [34], Janwa had posed this as an open problem and had shown that

$$(5.2) \qquad R(S_k(q)) \le q^{k-1} - 1.$$

The same bound was also obtained by Dodunekov [13] and Garg [19].

5.A.1 Lower Bounds on $R(S_k(q))$.

In [19], Garg has shown that the bound given by (5.2) is attained for k = 2 and q even and that the bound is not reached for k = 2 and q odd. He also improved this bound for q = 3 and 4 and obtained a lower bound on $R(S_k(q))$ (Proposition 2.16). Let q be odd and let $S_2(q)$ be the [q+1, 2, q] Simplex code generated by the matrix

$$G = \begin{bmatrix} 1 & 0 & 1 & \alpha_3 & \dots & \alpha_q \\ 0 & 1 & 1 & . & \dots & 1 \end{bmatrix} = \left[\begin{array}{c|c} 1 & \\ & G' \\ 0 & \end{array}\right]$$

Then G′ generates a [q,2,q-1] code C. By Theorem 3.1, R(C) = q-2. Therefore $R(S_2(q)) \ge q - 2$ and hence by Proposition 2.15 $R(S_2(q)) = q - 2$. This shows that the bound given by (5.2) is not reached for k = 2 and q odd.

Theorem 5.1. If q is odd, then $R(S_2(q)) = q - 2$.

Let C be an [n, k, d] code with generator matrix G. If $R = R(C) \le d$ and if $x \in F_q^n$ such that $d(x,C) = R$, then the matrix

$$G_1 = \left[\begin{array}{c|c} & \overset{\longleftarrow d-R \longrightarrow}{} \\ x & 11 \ldots 1 \\ \hline G & 0 \end{array}\right]$$

generates an [n + d - R, k + 1, d] code. Conversely, if C is an [n+s, k+1, d] code with s equivalent coordinates, then C is equivalent to a code generated by the matrix

$$G_2 = \left[\begin{array}{c|c} & \overset{\longleftarrow s \longrightarrow}{} \\ x & 1\ 1 \ldots 1 \\ \hline G' & 0 \end{array}\right]$$

for some $x \in F_q^n$. Clearly G′ generates an [n, k, d] code C with $R(C) \geq d - s$. This observation is useful in determining a lower bound on the covering radius of a code.

Remark 5.1. If C is an [n, k, d] code with $R = R(C) \leq d$, then there exists an [n + d - R, k + 1, d] code. Conversely, if there is an [n+s,k+1,d] code with s equivalent coordinates, then there exist an [n, k, d] code whose covering radius is at least d - s.

Theorem 5.2. i) If q is odd, then $R(S_3(q)) \geq q^2 - 3$.

ii) If q is even, then $R(S_3(q)) \geq q^2 - 2$.

Proof. Let q be odd. By Theorem 5.1, $R(S_2(q)) = q-2$. So there exists $x \in F_q^{q+1}$ with $d(x,S_2(q)) = q - 2$. The matrix

$$G' = \left[\begin{array}{c|c} x & 1\ 1 \\ \hline G_2(q) & 0 \end{array}\right]$$

generates a [q+3,3,q] code. Let C be a $[q^2+1,4,q(q-1)]$ two-weight code having a codeword of weight q^2 [8]. Then it has a generator matrix G″ of the form

$$(5.3) \qquad G'' = \left[\begin{array}{c|c} 1 & \\ 0 & A \\ 0 & \\ \hline 0 & 1\ 1\ \cdots\ 1 \end{array}\right]$$

The code D generated by the matrix

$$G = \left[\begin{array}{c|c} G' & \\ & G'' \\ 0 & \end{array}\right]$$

is a $[q^2 + q + 4, 4, q^2]$ code with three equivalent coordinates. Hence by Remark 5.1, there exists a $[q^2+q+1, 3, q^2]$ code whose covering radius is at least $q^2 - 3$. Since equivalent codes have same covering radius, $R(S_3(q)) \geq q^2 - 3$.

If q is even, then by Proposition 2.15, $R(S_2(q)) = q - 1$. Hence there exists $x \in F_q^{q+1}$ such that $d(x, S_2(q)) = q - 1$. The matrix

$$G''' = \left[\begin{array}{c|c} x & 1 \\ \hline G_2(q) & 0 \end{array}\right]$$

generates a $[q+2, 3, q]$ code C. Now the matrix

$$G = \left[\begin{array}{c|c} G''' & \\ & G'' \\ 0 & \end{array}\right]$$

generates a $[q^2+q+3, 4, q^2]$ code with two equal coordinates. Hence by Remark 5.1, there is a $[q^2+q+1, 3, q^2]$ code with covering radius greater than or equal to $q^2 - 2$. Since any $[q^2+q+1, 3, q^2]$ code is equivalent to $S_3(q)$, $R(S_3(q)) \geq q^2 - 2$.■

In [17], van Eupen has constructed a [43,5,27] ternary code with three equal coordinates. Without loss generality, we can assume that this code has a generator matrix of the form

$$G = \left[\begin{array}{c|c} 1\ 1\ 1 & x \\ 0 & G' \end{array}\right]$$

Then the matrix G' generates a [40, 4, 27] code with covering radius greater than or equal to 24. This proves the following theorem.

<u>**Theorem 5.3.**</u> $R(S_4(3)) \geq 24$.

If $(k,q-1) = 1$, then the Simplex code $S_k(q)$ is equivalent to a cyclic code C with generator polynomial $g(x) = \Sigma g_i x^i$, say, of degree $n - k$; $n = (q^k-1)/(q-1)$. Then the code consists of all cyclic shifts of g(x) and their scalar multiples, that is, $C = \{\alpha x^i g(x) \mid 0 \leq i < n,\ \alpha \in F_q\}$. For each $\alpha_i \in F_q$, let $n_i = |\{j \mid 0 \leq j \leq n-k \text{ and } g_j = \alpha_i\}|$. Since every nonzero codeword of C has weight q^{k-1}, $n_1 = n - q^{k-1} = (q^{k-1}-1)/(q-1)$. Therefore

$$R(C) \geq d(\underline{1},C) = \min\{\, n - n_i \mid 1 \leq i \leq q \,\},$$

where $\underline{1} = (1,1,\cdots,1)$. Thus we have

<u>**Theorem 5.4.**</u> If $(k, q-1) = 1$, then $R(S_k(q)) \geq n - \max\{\, n_i \mid 1 \leq i \leq q \,\}$.

To determine n_i's , we need to determine equations satisfied by them. Since the number of non-zero coefficients of the generator polynomial g(x) is q^{k-1},

$$n_2 + n_3 + \cdots + n_q = q^{k-1}. \tag{5.4}$$

Since the dual of the Simplex code is the Hamming code with distance three, strength of $S_k(q)$ is two. So for every pair of coordinate positions of $S_k(q)$ any q-ary ordered pair appears equal number of times. Thus if $(k, q-1)=1$,

$$\#(00)\text{-pair in the codeword list} = \binom{n}{2} + n(q-1)\binom{n_1}{2}$$

$$\#(11)\text{-pair in the codeword list} = n\left[\binom{n_2}{2} + \binom{n_3}{2} + \cdots + \binom{n_q}{2}\right]$$

Since the number of (00)-pair in the codeword list equals the number of (11)-pairs in the codeword list, the right hand side of the above equations are equal. Therefore

$$n\sum_{i=2}^{q}\frac{n_i(n_i - 1)}{2} = \frac{n(n-1)}{2} + \frac{n(q-1)n_1(n_1-1)}{2}$$

$$\sum_{i=2}^{q} n_i^2 = 2n - 2n_1 + n_1q^{k-1} - q^{k-1}$$

(5.5) $$\sum_{i=2}^{q} n_i^2 = \frac{q^{k-1}(q^{k-1} + q - 2)}{q - 1}.$$

If q = 3 and k is odd, then by solving equations (5.4) and (5.5), one gets

$$n_2 = \frac{1}{2}(3^{k-1} + \sqrt{3^{k-1}}) \text{ and } n_3 = \frac{1}{2}(3^{k-1} - \sqrt{3^{k-1}}).$$

Therefore $n - \max\{ n_2, n_3 \} = 3^{k-1} - \frac{1}{2}(\sqrt{3^{k-1}} + 1).$

If $q = 4$ and $3\nmid k$, the equations (5.4) and (5.5) become

$$n_2 + n_3 + n_4 = 2^{2k-2}$$

$$n_2^2 + n_3^2 + n_4^2 = 4^{k-1}.\frac{2}{3}(2^{2k-3}+1) = s.4^{k-1}.$$

For each $i = 2, 3, 4$, n_i must be even, say, $n_i = 2t_i$. Then t_2 +

$t_3 + t_4 = 2^{2k-3}$ and $t_2^2 + t_3^2 + t_4^2 = s.4^{k-2}$. Repeating this process $(k-1)$-times, we get $n_i = 2^{k-1}m_i$, where $m_2 + m_3 + m_4 = 2^{k-1}$ and $m_2^2 + m_3^2 + m_4^2 = s$. Since these equations have a solution, $3m_i \leq 2^{k-1} + 2$ for all $i = 2, 3, 4$. Hence

$$\max\{m_2, m_3, m_4\} \leq \begin{cases} \frac{1}{3}(2^{k-1} + 1) & \text{if } k \text{ even} \\ \frac{1}{3}(2^{k-1} + 2) & \text{if } k \text{ odd} . \end{cases}$$

Therefore by Theorem 5.4, we have

Theorem 5.5. i) If k is odd, then $R(S_k(3)) \geq 3^{k-1} - \frac{1}{2}(\sqrt{3^{k-1}} + 1)$.

ii) If $3 \nmid k$, then

$$R(S_k(4)) \geq \begin{cases} 4^{k-1} - \frac{1}{3}(2^{k-1} + 1) , & k \text{ even} \\ 4^{k-1} - (2^{k-1} + 2)/3 , & k \text{ odd.} \end{cases}$$

The lower bound given by the above theorem are much better than the bound given by Proposition 2.16. The idea of considering the Simplex code as a cyclic code and the proofs of Theorems 5.4 and 5.5(i) are due to an anonymous referee.

If $G_k(q)$ is a generator matrix for $S_k(q)$, then a generator matrix for $S_{k+1}(q)$ is given by the equation (5.1). Thus if $x \in F_q^n$ with $d(x, S_k(q)) = R(S_k(q))$, then the distance of the word $y = (x, 1, x, \cdots, x)$ from $S_{k+1}(q)$ clearly satisfies

$$d(y, S_{k+1}(q)) = \min\{ qR(S_k(q)) + 1, n(q-1)\} = qR(S_k(q)) + 1$$

where $n = (q^k-1)/(q-1)$. Hence by induction, we have the following following theorem.

Theorem 5.6. i) $R(S_{k+1}(q)) \geq qR(S_k(q)) + 1$.

ii) $R(S_m(q)) \geq q^{m-k} R(S_k(q)) + (q^{m-k}-1)/(q-1)$ whenever $m \geq k$.

5.A.2 Exact Covering Radius.

By (5.2), $R(S_3(q)) \leq q^2 - 1$. If $R(S_3(q)) = q^2-1$, then there exists an $x \in F_q^{q^2+q+1}$ such that $d(x, S_3(q)) = q^2-1$. So the matrix

$$G = \left[\begin{array}{c|c} 1 & x \\ \hline 0 & G_3(q) \end{array}\right]$$

generates a $[q^2+q+2, 4, q^2]$ code. This is a contradiction to the Corollary 4.3 and Theorem 4.6. Therefore, $R(S_3(q)) \leq q^2 - 2$ Hence by Theorem 5.2, we have

Theorem 5.7. i) If q is even, then $R(S_3(q)) = q^2 - 2$.

ii) If q is odd, then $q^2 - 3 \leq R(S_3(q)) \leq q^2 - 2$.

The bound given by the above theorem for odd q is best possible. In [19] Garg has shown that $R(S_3(3)) = 7$. Since $n_3(5,27) \geq 43$ [30], $b_3(4,27) \geq 3$. So by Proposition 2.14 $R(S_4(3)) \leq 24$ and hence by Theorem 5.5, we have

Theorem 5.8. $R(S_4(3)) = 24$.

By Theorem 5.5, $R(S_4(4)) \geq 61$. If $R(S_4(4)) = 62$, then there exists a $x \in F_4^{85}$ such that $d(x, S_4(4)) = 62$. The matrix

$$G = \left[\begin{array}{cc|c} 1 & 1 & x \\ \hline 0 & 0 & \\ \vdots & \vdots & G_4(4) \\ 0 & 0 & \end{array}\right]$$

generates a $[87,5,64]$ code over F_4 . But such a code does not exist as by Theorem 4.15 $n_4(5,64) \geq 88$. Hence we have

Theorem 5.9. $R(S_4(4)) = 61$.

As an immediate Corollary we have

Corollary 5.1. $n_4(5, 64) = 88$.

Proof. By Theorem 4.14, $n_4(5,64) \geq 88$. Since $R(S_4(4)) = 61$, there exists a $x \in F_q^{85}$ such that $d(x,S_4(4)) = 61$. Therefore the matrix

$$G = \left[\begin{array}{c|c} 1\ 1\ 1 & x \\ \hline 0 & G_4(4) \end{array}\right]$$

generates a $[88, 5, 64]$ quaternary code. Hence $n_4(5,64) = 88$.∎

5.A.3 Upper Bounds on $R(S_k(q))$.

The following theorem gives a better upper bound for $R(S_m(q))$ if $R(S_k(q))$ is known for some k, $k \leq m$.

Theorem 5.10. If for some k and q, $R(S_k(q)) \leq q^{k-1} - t$, $t \geq 1$, then $R(S_m(q)) \leq q^{m-1} - t$ for all $m \geq k$.

Proof. Let $m = k + 1$ and let $G_{k+1}(q)$ be the generator matrix of $S_{k+1}(q)$ given by (5.1). $G_{k+1}(q)$ is equivalent to the matrix

$$G'_{k+1}(q) = \left[\begin{array}{c|c} 0\ 0\ \ldots\ 0 & \overbrace{1\ 1\ \ldots\ 1}^{q^k} \\ \hline G_k(q) & D \end{array}\right].$$

Since equivalent codes have same covering radius, by (2.8)

$$R(S_{k+1}(q)) \leq R(S_k(q)) + R(\text{repetition code of length } q^k)$$

$$\le q^{k-1} - t + (q-1)q^k/q = q^k - t.$$

Hence by induction on m the theorem follows.■

If q is odd, by Theorems 5.7 and 5.10, we get the following upper bound for $S_k(q)$ that is better than the bound given by (5.2).

Corollary 5.2. $R(S_k(q)) \le q^{k-1} - 2$ for all $k \ge 3$.

Corollary 5.3. For $k \ge 3$, $n_q(k+1,q^{k-1}) > g_q(k+1,q^{k-1})$.

Proof. If not, then $n_q(k+1,q^{k-1}) = g_q(k+1,q^{k-1}) = g_q(k,q^{k-1}) + 1 = n_q(k, q^{k-1}) + 1$. So $b_q(k,q^{k-1}) = 1$. By Proposition 2.14, there exists a $[(q^k-1)/(q-1),k,q^{k-1}]$ code with covering radius $q^{k-1}- 1$. Since equivalent codes have same covering radius, $R(S_k(q)) = q^{k-1}-1$, a contradiction to Corollary 5.2.■

If q = 3 or 4, the following theorems, the proof of which follows from Theorems 5.8, 5.9 and 5.10, further improve the bound given by Corollary 5.2.

Theorem 5.11. If $q = 3, 4$, then $R(S_k(q)) \le q^{k-1} - 3$ for all $k \ge 4$.

5.B THE COVERING RADIUS OF THE MACDONALD CODES.

Let $1 \le u < k$ be given integer. Recall that a MacDonald code $C_{k,u}(q)$ is a $[(q^k-q^u)/(q-1),\ k,\ q^{k-1} -q^{u-1}]$ code generated by th matrix

$$(5.6) \qquad G_{k,u}(q) = \left[G_k(q) \;\backslash\; \left[\frac{0}{G_u(q)} \right] \right]$$

where $G_m(q)$ is a generator matrix of the Simplex code $S_m(q)$, 0 is a $(k-u) \times (q^u-1)/(q-1)$ null matrix and $[A\backslash B]$ is a matrix obtained from A by deleting the columns of the matrix B. In [19], Garg has shown that $R(C_{k,2}(2)) = 2^{k-1} - 4$ for $k \geq 4$. In fact we can easily find out the covering radius for $k = 3$. Observe that $C_{3,2}(2)$ is a [4, 3, 2] code generated be the matrix

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

By Singleton bound, $R(C_{3,2}(2)) \leq 1$. Since $C_{3,2}(2)$ is a proper subset of the whole space, $R(C_{3,2}(2)) \geq 1$. Hence $R(C_{3,2}(2)) = 1$. For $q > 2$, almost nothing is known about the covering radius of $C_{k,u}(q)$. Since $C_{k,u}(q)$ is a code meeting the Griesmer bound, $R(C_{k,u}(q)) \leq q^{k-1} - q^{u-1} - 1$. In this section we improve this bound and determine lower bounds for the covering radius of $C_{k,u}(q)$ in general and use them to determine exact covering radius of small values of k, u and q.

5.B.1 Lower Bounds on $R(C_{k,u}(q))$.

The Matrix (5.6) can be written as

$$G_{k,u}(q) = \left[\begin{array}{c|c} G_{k,k-1}(q) & G_{k-1,u}(q) \end{array}\right]$$

and hence by (2.9),

$$R(C_{k,u}(q)) \geq R(C_{k,k-1}(q)) + R(C_{k-1,u}(q)) \tag{5.7}$$

In [17] van Eupen has constructed a [29,5,18] ternary code C with two equal coordinates. A generator matrix for C can be written in the form

$$G = \left[\begin{array}{c|c} 1\ 1 & x \\ \hline 0 & G' \end{array}\right].$$

Then the matrix G′ generates a [27, 4, 18] code C′ and $d(x, C') = 16$. Therefore $R(C') \geq 16$. Since any [27,4,18] code is equivalent to $C_{4,3}(3)$, $R(C_{4,3}(3)) \geq 16$. Thus by inequality (5.7), we have

Theorem 5.12. $R(C_{4,3}(3)) \geq 16$ and $R(C_{4,u}(3)) \geq R(C_{3,u}(3)) + 16$.

Theorem 5.13. $R(C_{3,1}(q)) \geq q^2 - 3$.

Proof. Let A be a $[q^2+1,\ 4,\ q^2-q]$ code with two nonzero weights q^2-q and q^2 [8]. Without loss of generality we can choose a generator matrix of the form

$$G_A = \left[\begin{array}{c|c} 0 & 1\ 1\ \ldots .1 \\ \hline 1 & x \\ 0 & x' \\ 0 & x'' \end{array}\right]$$

where $x, x', x'' \in F_q^{q^2}$. Let B be a $[q+1,\ 3,\ q-1]$ code guarantee by Proposition 2.18. A generator matrix of B is of the form

(5.8) $$G_B = \begin{bmatrix} 1 & y \\ 0 & y' \\ 0 & y'' \end{bmatrix}$$

where $y, y', y'' \in F_q^q$. Then the matrix

$$G = \left[\begin{array}{c|c} x' & y' \\ x'' & y'' \\ 1\ 1\ .\ .\ .\ 1 & 0\ .\ .\ .\ 0 \end{array}\right]$$

generates a $[q^2 + q, 3, q^2 - 1]$ code C and $d((x,y), C) = q^2 - 3$. Since any code with these parameters is equivalent to $C_{3,1}(q)$, $R(C_{3,1}(q)) \geq 3$.

5.B.2 UPPER BOUNDS ON $R(C_{k,u}(q))$.

The code $C_{k,u}(q)$ is a code that meets Griesmer bound. Hence

(5.9) $$R(C_{k,u}(q)) \leq q^{k-1} - q^{u-1} - 1.$$

Multiplying columns of $G_{k,u}(q)$ by suitable nonzero elements of F_q , we find that $C_{k,u}(q)$ is equivalent to the code generated by the matrix.

$$\begin{array}{c} \begin{array}{cc} \leftarrow q^{k-1} \rightarrow & \phantom{G_{k-1,u}(q)} \end{array} \\ \left[\begin{array}{c|c} 1\ 1\ .\ .\ .\ 1 & 0\ 0\ .\ .\ .\ 0 \\ \hline A & G_{k-1,u}(q) \end{array}\right] \end{array}$$

Hence by (2.18), $R(C_{k,u}(q)) \leq q^{k-2}(q-1) + R(C_{k-1,u}(q))$. Repeatin this (k-m)-times, $u < m \leq k-1$ we get

$$R(C_{k,u}(q)) \leq q^{k-2}(q-1) + q^{k-3}(q-1) + \ldots + q^{m-1}(q-1) + R(C_{m,u}(q)$$

Therefore

$$(5.10) \qquad R(C_{k,u}(q)) = q^{m-1}(q^{k-m} - 1) + R(C_{m,u}(q)).$$

In particular if $m = u + 1$, we have

$$(5.11) \qquad R(C_{k,u}(q)) \le q^{k-1} - q^{u} + R(C_{u+1,u}(q)).$$

In case $u \ge 3$, the following theorem improves the bound given by (5.9).

Theorem 5.14. $R(C_{k,u}(q)) \le q^{k-1} - q^{u-1} - 2$ for $u \ge 3$.

Proof. Since $C_{u+1,u}(q)$ is an optimal code, $R(C_{u+1,u}(q)) \le q^{u} - q^{u-1} - 1$. If $R(C_{u+1,u}(q)) = q^{u} - q^{u-1} - 1$, then there exists $y \in F_q^n$, $n = (q^k - q^u)/(q-1)$, with $d(y, C_{u+1,u}(q)) = q^u - q^{u-1} - 1$. The matrix

$$G = \left[\begin{array}{c|c} y & 1 \\ \hline G_{u+1,u}(q) & 0 \end{array}\right]$$

generates a $[q^u+1,\ u+2,\ q^u-q^{u-1}]$ code C. Let $1 \le i \le q^{u-1} - 1$ and let $w = q^u - q^{u-1} + i$. If $A_w \ne 0$, then by Proposition 2.9, Res(C,w) is a $[q^{u-1} + 1 - i,\ u+1,\ q^{u-2}(q-1) + \lceil \frac{i}{q} \rceil - i]$ code. Hence by (2.4),

$$\begin{aligned} q^{u-1}+1-i &\ge \sum_{j=0}^{u} \left\lceil \frac{q^{u-2}(q-1) - \lceil i(q-1)/q \rceil}{q^j} \right\rceil \\ &\ge \sum_{j=0}^{u-2} \left(q^{u-2}(q-1) - \frac{i(q-1)}{q^{j+1}}\right) + 2 \\ &= q^{u-1} + 1 - i + i/q^{k-1}, \end{aligned}$$

a contradiction. Therefore possible nonzero weights in C are $d = q^u - q^{u-1}$, $n - 1$ and $n = q^u + 1$. By Proposition 2.5, $B_1 = B_2 = 0$.

The MacWilliams identities (2.3) give

$$A_d + A_{n-1} + A_n = q^{u+2} - 1$$

$$(q^{u-1}+1)A_d + A_{n-1} = (q^{u+1}-1)n$$

$$((q^{u-1}+1)q^{u-1}/2)A_d = (q^u-1)n(n-1)/2$$

Solving these equations we get $A_n = (q-1)q^{u+1}(1-q^{u-2})/(q^{u-1}+1)$. If $u \geq 3$ then $A_n < 0$, a contradiction. Thus for $u \geq 3$, $R(C_{u+1,u}(q)) \leq q^u - q^{u-1} - 2$. Substituting this in (5.11) we proved.■

Using Theorem 5.14 and Theorem 5.12, we get immediately

Corollary 5.4. $R(C_{4,3}(3)) = 16$.

Thus bound given by Theorem 5.14 is best possible.

Theorem 5.15. $R(C_{3,1}(q)) = q^2 - 3$.

Proof. Suppose $R(C_{3,1}(q)) = q^2 - 2$. Then there exists $x \in F_q^{q^2+q}$ such that $d(x, C_{3,1}(q)) = q^2 - 2$. So the matrix

$$G = \begin{bmatrix} x \\ G_{3,1}(q) \end{bmatrix}$$

generates a $[q^2 + q, 4, q^2 - 2]$ code. But by Theorem 4.4, such a code does not exist. Therefore $R(C_{3,1}(q)) \leq q^2 - 3$ and hence by Theorem 5.13, $R(C_{3,1}(q)) = q^2 - 3$.■

Using inequality (5.10) and Theorem 5.15, we get the following improvement

Corollary 5.5. $R(C_{k,1}(q)) \leq q^{k-1} - 3$ for $k \geq 3$.

Theorem 5.16. $R(C_{4,2}(q))) \leq q(q^2-1) - 2$.

Proof. Suppose $R(C_{4,2}(q)) = q(q^2-1)-1$. Then there is a $x \in F_q^{q^3+q^2}$ with $d(x, C_{4,2}(q)) = q(q^2-1)-1$. The matrix

$$G = \left[\begin{array}{c|c} 1 & x \\ \hline 0 & \\ \vdots & G_{4,2}(q) \\ 0 & \end{array}\right]$$

generates a $[q^2(q+1)+1, 5, q(q^2-1)]$ code C. So by Proposition 2.9, a $[q^2+q+1, 4, q^2-1]$ code exists, but by Theorem 4.4 such a code does not exist. This proves the Theorem.■

By inequality (5.10) and Theorem 5.16, we have

Corollary 5.6. $R(C_{k,2}(q)) \le q^{k-1} - q - 2$ for $k \ge 4$.

Since $n_q(4,q^2-q) = q^2+1$ [8] and $n_q(3,q^2-q) = q^2$, $b_q(3,q^2-q) = 1$. Therefore by Proposition 2.14, there exists a $[q^2, 3, q^2-q]$ code with covering radius $q^2 - q - 1$. Since any code with these parameters is equivalent to the MacDonald code $C_{3,2}(q)$ and equivalent code have same covering radius, we have the following

Theorem 5.17. $R(C_{3,2}(q)) = q^2 - q - 1$.

Let $q = 3$. By inequality (5.10), Corollary 5.6 and Theorem 5.17 we have $21 \le R(C_{4,2}(3)) \le 22$. By Theorem 5.8, $R(C_{4,1}(3)) \ge 23$. If $R(C_{4,1}(3)) \ge 24$, then there is a $x \in F_3^{29}$ such that $d(x, C_{4,1}(3)) = 24$. Then the matrix

$$G = \left[\begin{array}{cc|c} 1 & 1 & x \\ & 0 & G_{4,1}(3) \end{array}\right]$$

generates a [41,5,26] ternary code, a contradiction to $n_3(5,26) =$

42 [33]. This proves

Theorem 5.18. $R(C_{4,1}(3)) = 23$ and $21 \le R(C_{4,2}(3)) \le 22$.

By inequality (5.10) and Theorem 5.18, we get the following improvement of Corollary 5.5

Corollary 5.7. $R(C_{k,1}(3)) \le 3^{k-1} - 4$ for $k \ge 4$.

Using Theorem 5.14, Corollaries 5.5 and 5.6, we get the following improvement to (5.9)

$$R(C_{k,u}(q)) \le q^{k-1} - q^{u-1} - 2 \text{ for } k \ge 4. \tag{5.12}$$

Theorem 5.19. $n_q(k+1, q^{k-1} - q^{u-1}) \ge g_q(k+1, q^{k-1} - q^{u-1}) + 1$ for $k \ge 4$.

Proof. Suppose $n_q(k+1, q^{k-1} - q^{u-1}) = g_q(k+1, q^{k-1} - q^{u-1})$ for $k \ge 4$. Then $b_q(k, q^{k-1} - q^{u-1}) = 1$ because $n_q(k, q^{k-1} - q^{u-1}) = (q^k - q^u)/(q-1)$. Therefore by Proposition 2.14, there is a $[(q^k - q^u)/(q-1), k, q^{k-1} - q^{u-1}]$ code with covering radius $q^{k-1} - q^{u-1} - 1$ for $k \ge 4$, a contradiction to the inequality (5.12). Hence proved.∎

Since $C_{4,2}(4)$ is a [80, 4, 60] quaternary code, by Theorem 4.10, $b_4(4,60) \ge 2$. Therefore by Proposition 2.14, $R(C_{4,2}(4)) \le 58$ and hence by the inequality (5.10), $R(C_{k,2}(4)) \le 4^{k-1} - 6$.

Using MacDonald code we can give another lower bound to Simplex code. The generator matrix of $S_k(q)$ is equivalent to the matrix

$$G = \left[\begin{array}{c|c} 0 \; . \; . \; . \; 0 & \\ & G_{k,k-1}(q) \\ G_{k-1}(q) & \end{array}\right]$$

Then

$$(5.13) \qquad R(S_k(q)) \geq R(S_{k-1}(q)) + R(C_{k,k-1}(q))$$

This bound is better than the bound given by Theorem 5.6. For example, by Theorem 5.2 and Theorem 5.17, the inequality (5.13) gives $R(S_3(q)) \geq q - 2 + q^2 - q - 1 = q^2 - 3$ for q odd but the Theorem 5.6 gives $R(S_3(q)) \geq q^2 - 2q + 1$ for q odd. Definitely the bound given by (5.13) is better than the bound given by Theorem 5.6 provided we know the covering radius of MacDonald code.

References

1. L. D. Baumert and R. J. McEliece, "A note on the Griesmer bound", IEEE Trans. Inform. Theory, Vol. IT-19, pp. 134-135, 1973.

2. B. I. Belov, "A conjecture on the Griesmer bound", Optimization Methods and Their Applications, All-Union Summer Sem., Lake Baikal, 1972.

3. B. I. Belov, V. N. Logachev and V. P. Sandimirov, "Construction of a class of linear binary codes that meet the Varshamov-Griesmer bound", Probl. of Info. Transmission, Vol. 10, No. 3, pp. 211-217, 1974.

4. M. C. Bhandari and M. S. Garg, "A Note on the Covering Radius of optimum Codes", Discrete Applied Mathematics, Vol. 33, pp. 3-9, 1990.

5. M. C. Bhandari and M. S. Garg, "Optimum codes of dimension 3 and 4 over GF(4)", IEEE Trans. Inform. Theory, Vol. 38, pp. 1564-1567, 1992.

6. R. A. Brualdi, V. S. Pless and R. M. Wilson, "Short codes with a given covering radius", IEEE Trans. Inform. Theory, Vol. 35 pp. 99-109, 1989.

7. P. B. Busschbach, M. G. L. Gerretzen and H.C.A. van Tilborg", On the Covering radius of binary linear codes meeting the Griesmer bound", IEEE Trans. Inform. Theory, Vol. IT-31, pp. 465-468, 1985.

8. A. R. Calderbank and W. M. Kantor, "The geometry of two weigh codes", Bull. Lon. Math. Soc., Vol. 18, pp. 97-122, 1986.

9. A. R. Calderbank and N. J. A. Sloane, "Inequalities f covering codes", IEEE Trans. Inform. Theory, Vol. 34, p 1276-1280, 1988.

10. W. Chen and I. S. Honkala, "Lower Bounds for q-ary Coveri codes", IEEE Trans. Inform. Theory, Vol. 36, No. 3, p 664-671, 1990.

11. G. D. Cohen, M. R. Karpovsky, H. F. Mattson, Jr., and J.

Schatz, "Covering Radius-Survey and Recent Results", IEEE Trans. Inform. Theory, Vol. IT-31, pp. 328-343, 1985.

12. G. D. Cohen, A. C. Lobstein, and N. J. A. Sloane, "Further Results on the Covering radius of codes", IEEE Trans. Inform. Theory, Vol. IT-32, No. 5, pp. 680-694, 1986.

13. P. Delsarte, "Four fundamental parameters of a code and their combinatorial significance", Inform. and Contr., Vol. 23 pp. 407-438, 1973.

14. S. M. Dodunekov, "Minimum block length of a linear q-ary code with specified dimension and code distance", Probl. of Inform. Transmission, Vol. 20, pp. 239-249, 1984.

15. S. M. Dodunekov, T. Helleseth, N. Manev and ø. Ytrehus, "New bounds on binary linear codes of dimension eight", IEEE Trans. Inform. Theory, Vol. IT-33, pp. 917-919, 1987.

16. S. M. Dodunekov and N. L. Manev, "An improvement of the Griesmer bound for some small minimum distances", Discrete Appl. Math., Vol. 12, pp. 103-114, 1985.

17. M. van Eupen , "Five New optimal Ternary linear codes", IEEE Trans. Inform. Theory, Vol. 40, No. 1, pp. 193, 1994.

18. P. G. Farrell, "Linear binary anticodes", Electronics Letters, Vol. 6, pp. 419-421, 1970.

19. M. S. Garg, "On Optimum codes and Their covering radii", Ph. D Thesis, IIT Kanpur(India), 1990.

20. R. L. Graham and N. J. A. Sloane, "On the covering radius of codes", IEEE Trans. Inform. Theory, Vol. IT-31, pp. 385-401, 1985.

21. P. P. Greenough and R. Hill, "Optimal linear codes over GF(4)" Discrete Mathematics, Vol. 125, pp. 187-199, 1994.

22. J. H. Griesmer, "A bound for error-correcting codes", IBM J. Res. Develop., Vol. 4, pp. 532-542, 1960.

23. N. Hamada, "Characterization of Min. Hypers in a finite projective geometry and its applications to error-correcting codes", Bull. Osaka Women's Univ., Vol. 24, pp. 1-23, 1987.

24. N. Hamada and M. Deza, "Characterization of 2(q + 1) +2, 2; t, q-Min. Hypers in PG(t,q) (t ≥ 3, q ≥ 5) and its applications to

error-correcting codes", Discrete Math., Vol. 71, pp. 219-231, 1988.

25. N. Hamada and T. Helleseth, "A Characterization of some Min. Hypers in a finite projective geometry PG(6, 4)", Europ. J. Combinat., Vol. 11, pp. 541-548, 1990.

26. N. Hamada and F. Tamari, "Construction of optimal codes and optimal fractional factorial designs using linear programming", Ann. Discrete Math., Vol. 6, pp. 175-188, 1980.

27. H. Hamalainen and S. Rankinen, "Upper Bounds for football pool problems and mixed covering codes", J. Combin. Theory, Ser. A, Vol. 56, pp. 84-95, 1991.

28. T. Helleseth and ø. Ytrehus, "New bounds on the minimum length of binary linear block codes of dimension 8", Reports in Informatics, Departments of Informatics, University of Bergen, Norway, Report No. 21, 1986.

29. R. Hill, "Optimal linear codes", In Cryptography and Coding II, edited by C. Mitchell, Oxford Univ. Press, pp. 75-104, 1991.

30. R. Hill and D. E. Newton, "Optimal ternary linear codes", Designs, Codes and Cryptography, Vol. 2, pp. 137-157, 1992.

31. I. S. Honkala, "Lower Bounds for Binary Covering codes", IEEE Trans. Inform. Theory, Vol. 34, pp. 326-329, 1988.

32. I. S. Honkala, "On (k,t)-subnormal covering codes", IEEE Trans. Inform. Theory, Vol. 37, No. 4, pp. 1203-1206, 1991.

33. H. Janwa, "Some optimal codes from Algebraic geometry and their covering radii", Europ. J. Combinatorics, Vol. 11, pp. 249-266, 1988.

34. H. Janwa, "Some new upper bounds on the covering radius of binary linear codes", IEEE Trans. Inform. Theory, Vol. IT-35, pp. 110-122, 1989.

35. H. Janwa, "On the covering radius of q-ary codes", Proceedings of AAECE-7, 1991.

36. J. G. Kalbfleisch and R. G. Stanton, "A combinatorial problem

in matching", J. London Math. Soc., Vol 44, No. 1, pp. 60-64, 1969 and Vol. 1, No. 2, pp. 398, 1969.

37. H. J. L. Kamps and J. H. van Lint, "The football pool problem for 5 matches", J. Combin. Theory, Vol. 3, pp. 315-325, 1967.

38. J. H. van Lint Jr. and G. J. M. van Wee, "Generalized Bounds on Binary/Ternary mixed Packing and covering codes", J. Combin Theory, Ser. A, Vol. 57, pp. 130-143, 1991.

39. A. C. Lobstein and G. J. M. van Wee, "On Normal and subnormal q-ary covering codes", IEEE Trans. Inform. Theory, Vol. 35, No. 6, pp. 1291-1295, 1989.

40. V. N. Logacev, "An improvement of Griesmer bound in the case of small code distance", Optimization Methods and Their Applications, All-Union Summer Sem., Lake Baikal, pp. 107-111, 1972.

41. J. E. MacDonald, "Design methods for maximum minimum-distance error-correcting codes", IBM J. Res. Develop., Vol. 4, pp. 34-37, 1960.

42. F. J. MacWilliams, "A theorem on the distribution of weights in a systematic code", Bell. Syst. Tech. J, Vol. 42, pp. 79-94, 1963.

43. F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting codes, Amsterdam, North Holland, 1977.

44. E. Mattioli, "Sopra una Particolare proprieta dei gruppi abeliani finiti", Ann. Scuola Norm. Sup. Pisa, Vol. 3, No. 3, pp. 59-65, 1950.

45. H. F. Mattson Jr., "An improved upper bound on covering radius", Lecture Notes in Computer Science, Springer, Vol. 228 pp. 90-106, 1986.

46. J. G. Mauldon, "Covering theorems for groups", Quart. J. Math. Oxford, Ser. 2, Vol. 1, pp. 284-287, 1950.

47. P. R. J. Ostergard, "Upper bounds for q-ary covering codes", IEEE Trans. Inform. Theory, Vol. 37, No. 3, pp. 660-664, 1991.

48. P. R. J. Ostergard, "Construction Methods for covering codes", Helsinki University of Tech., Digital Systems Lab., 1993.

linear codes with large minimum

distance", IEEE Trans. Inform. Theory, Vol. 21, No. 1, pp. 106-110, 1975.

50. V. Pless, Introduction to the Theory of error-correcting codes, Wiley, New York. 1989.

51. E. R. Rodemich, "Coverings by rook domains", J. Combin. Theory, Ser. A, Vol. 9, pp. 117-128, 1970.

52. C. E. Shannon, "A Mathematical theory of communication", Bell Syst. Tech. J., Vol. 27, pp. 379-423 & 623-656, 1948.

53. G. Solomon and J. J. Stiffler, "Algebraically punctured cyclic codes", Inform. and Contr., Vol. 8, pp. 170-179, 1965.

54. R. G. Stanton, J. D. Horton, and J. G. Kalbfleisch, "Covering theorems for vectors with special reference to the case of four and five components", J. London Math. Soc., Vol. 1, pp. 493-499, 1969.

55. R. G. Stanton and J. G. Kalbfleisch, "Covering problems for dichotomized matchings", Aequationes Math., Vol. 1, pp. 94-103, 1968.

56. R. G. Stanton and J. G. Kalbfleisch, "Intersection inequalities for the covering problem", SIAM J. Appl. Math. Vol. 17, pp. 1311-1316, 1969.

57. R. Struik, "On the structure of linear codes with covering radius two and three", IEEE Trans. Inform. Theory, Vol. 40, No. 5, pp. 1406-1416, 1994.

58. O. Taussky and J. Todd, "Covering theorems for groups", Ann. Soc. Polon. Math, Vol. 21, pp. 303-305, 1948.

59. H. C. A. van Tilborg, "The smallest length of binary 7-dimensional linear code with prescribed minimum distances", Discrete Math., Vol. 33, pp. 197-207, 1981.

60. A. E. Brouwer and T. Verhoeff, "An updated table of minimum distance bounds for binary linear codes", IEEE Trans. Inform. Theory, Vol. 39. pp. 662-677, 1993.

61. G. J. M. van Wee, "Improved Sphere Bounds on the covering radius of codes", IEEE Trans. Inform. Theory, Vol. 34, pp. 237-245, 1988.

62. G. J. M. van Wee, "Bounds on packings and coverings by spheres

in q-ary and mixed Hamming spaces", J. of Combinat. Theory, Ser. A, Vol. 57, pp. 117-129, 1991.

63. S. K. Zaremba, "A Covering theorem for Abelian groups", J. London Math. Soc., Vol. 26, pp. 71-72, 1950.

64. A. Cossu, "Su alcune proprieta dei$\{k;n\}$ – archi di un piano Proiettiro sopra un corpo finito", Rend. Mat. e appl., Vol. 20, pp. 271-277, 1961.

65. R. Daskalov, "Two nonexistance results for Quaternary linear codes of dimension five", Proc. Int. Workshop on Optimal Codes Sozopol, Bulgaria, pp. 40-44, 1995.

66. R. Daskalov and E. Metodieva, "The non-existance of some 5-dimensional quaternary linear codes", IEEE Trans. Inform. Theory Vol. 41, pp. 581-583, 1995.

67. N. Hamada, "The non-existence of some quaternary linear codes meeting the Griesmer bound and the bounds for $n_4(5,d)$, $1 \leq d \leq 256$", Math Japonica, Vol. 43, pp. 7-21, 1996.

68. R. Hill, Landgev and Lizak, "Optimal quaternary codes of dimension 4 and 5 ", Proc. Fourth Inter. Work shop : Algebraic and Combinatorial Coding Theory, Novgorod, Russia, pp. 98-101, 1994.